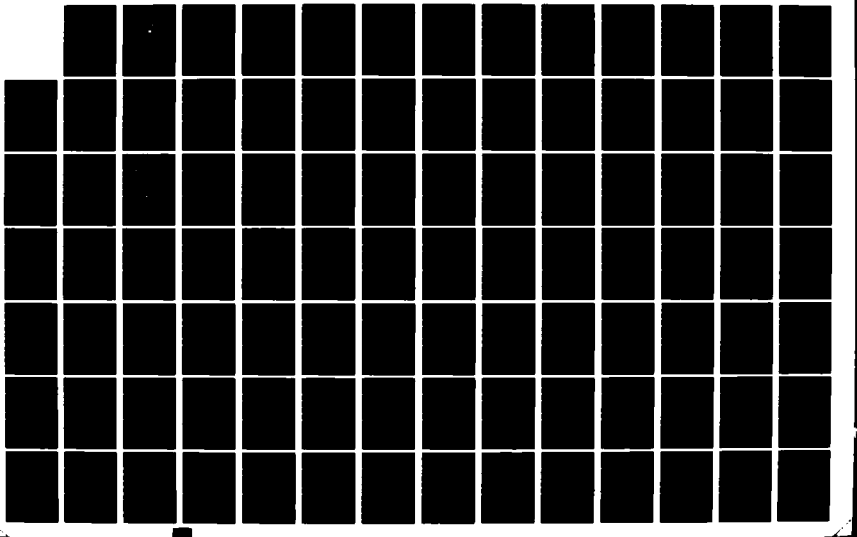
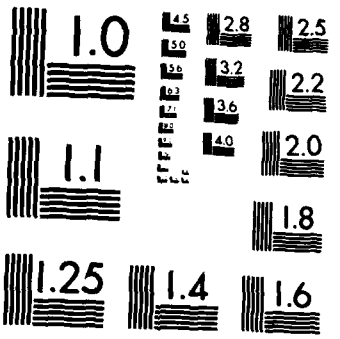
AD-A127 631 PROPOSAL FOR STOCK POINT LOGISTICS INTEGRATED COMMUNICATIONS ENVIRONMENT (.. (U) NAVAL POSTGRADUATE SCHOOL MONTEREY CA S K CROWDER ET AL. DEC 82 1/2

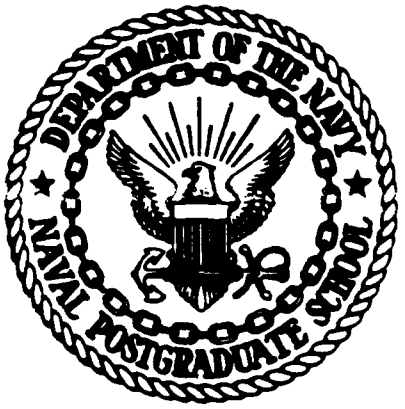
UNCLASSIFIED F/G 15/3 NL





MICROCOPY RESOLUTION TEST CHART
NATIONAL BUREAU OF STANDARDS-1963-A

NAVAL POSTGRADUATE SCHOOL
Monterey, California



THESIS

PROPOSAL FOR STOCK POINT LOGISTICS INTEGRATED COMMUNICATIONS ENVIRONMENT (SPLICE) LOCAL AREA NETWORK RISK MANAGEMENT

by

Sharron K. Crowder
Jan M. Adams
December, 1982

Thesis Advisor: Norman F. Schneidewind

Approved for Public Release; Distribution Unlimited

DTIC FILE COPY

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

REPORT DOCUMENTATION PAGE		READ INSTRUCTIONS BEFORE COMPLETING FORM
1. REPORT NUMBER	2. GOVT ACCESSION NO. AD-A127631	3. RECIPIENT'S CATALOG NUMBER
4. TITLE (and Subtitle) Proposal for Stock Point Logistics Integrated Communications Environment (SPLICE) Local Area Network Risk Management		5. TYPE OF REPORT & PERIOD COVERED Master's Thesis December, 1982
		6. PERFORMING ORG. REPORT NUMBER
7. AUTHOR(s) Sharron K. Crowder Jan M. Adams		8. CONTRACT OR GRANT NUMBER(s)
9. PERFORMING ORGANIZATION NAME AND ADDRESS Naval Postgraduate School Monterey, California 93940		10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS
11. CONTROLLING OFFICE NAME AND ADDRESS Naval Postgraduate School Monterey, California 93940		12. REPORT DATE December, 1982
		13. NUMBER OF PAGES 120
14. MONITORING AGENCY NAME & ADDRESS(if different from Controlling Office)		15. SECURITY CLASS. (of this report) UNCLASSIFIED
		15a. DECLASSIFICATION/DOWNGRADING SCHEDULE

16. DISTRIBUTION STATEMENT (of this Report)

Approved for Public Release; Distribution Unlimited

17. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, if different from Report)

18. SUPPLEMENTARY NOTES

19. KEY WORDS (Continue on reverse side if necessary and identify by block number)

Risk Management, ADP Security, SPLICE

20. ABSTRACT (Continue on reverse side if necessary and identify by block number)

The SPLICE system is designed to integrate a variety of current and projected NAVSUP processing and telecommunications applications. The operation of the more than twenty new applications systems currently under development will increase the Navy's dependence on automated support, and will require that the risk of operating the SPLICE data processing environment be evaluated and managed at an acceptable level. This thesis identifies the requirements for implementing a Risk Management Program, provides (Continued)

DD FORM 1 JAN 73 1473 EDITION OF 1 NOV 65 IS OBSOLETE
S/N 0102-014-6601

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

ABSTRACT (Continued) Block # 20

a formal model for the quantification and management of risk, and examines contemporary technical and managerial countermeasures which could be effective in reducing the operational risk of SPLICE.

DTIC
COPY
INSPECTED
2

Approved for public release; distribution unlimited.

Proposal for Stock Point Logistics Integrated Communications Environment (SPLICE) Local Area Network Risk Management

by

Sharron K. Crowder
Lieutenant, United States Navy
B.A., University of Texas, 1977

Submitted in partial fulfillment of the requirements for the degree of

MASTER OF SCIENCE IN COMPUTER SCIENCE

and

Jan M. Adams
Lieutenant, United States Navy
B.S., Sam Houston State University, 1975

Submitted in partial fulfillment of the requirements for the degree of

MASTER OF SCIENCE IN INFORMATION SYSTEMS

from the

NAVAL POSTGRADUATE SCHOOL
December 1982

Authors: Sharron K. Crowder

Jan M. Adams

Approved by: Norman F. Schneidewind
Thesis Advisor

Second Reader

Chairman, Department of Computer Science

Chairman, Department of Administrative Sciences

Dean of Information and Policy Sciences

ABSTRACT

The SPLICE system is designed to integrate a variety of current and projected NAVSUP processing and telecommunications applications. The operation of the more than twenty new applications systems currently under development will increase the Navy's dependence on automated support, and will require that the risk of operating the SPLICE data processing environment be evaluated and managed at an acceptable level. This thesis identifies the requirements for implementing a Risk Management Program, provides a formal model for the quantification and management of risk, and examines contemporary technical and managerial countermeasures which could be effective in reducing the operational risk of SPLICE.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

I. BACKGROUND

A. INTRODUCTION TO RISK MANAGEMENT

Computers have become an integral part of the business and government world by performing many of the operations and applications that, in the past, were either done manually or not at all. In addition to spending vast sums of money to acquire and operate computer hardware, Navy activities have funded system and application software development, communication links for remote terminals and networks, site construction and daily operating expenses, and the administrative overhead of a data processing department staff. More importantly, the proliferation of computers has affected the day-to-day operations at a number of Navy activities. Many activities depend so heavily on their computers that if the computers ceased operation, either the activities would fail to accomplish their mission or they would suffer a severe degradation in their mission effectiveness.

The introduction of automation has resulted in a substantial increase in the risk an activity faces. For example, the centralization of data and services is often associated with a remote access capability. This added capability permits interrogation and alteration of data files with little or no check on the authenticity of the source. Additionally, there is often a reduction in the accessibility of visual records accompanying the shift to automated support. In a manual system, sales ledgers, payment books, and invoices are maintained by various internal departments to manage and monitor an activity's business. In a computerized system, these same records are

retained on magnetic storage media and are updated automatically by a software program. The accuracy and authenticity of these records has become the joint responsibility of the data processing department and the user, which often results in uncertainty about the responsibility for data integrity. The question is who is responsible for the data -- the user who originates the input and uses the result, or the data processing department, which has day-to-day responsibility for the automated processing. These new risks have generated an obligation of management to protect this significant investment and to provide for continuity of operations should a catastrophe or accident occur. [Ref. 1: pp. 1-8]

Protection can be accomplished by designing, developing and implementing countermeasures. These countermeasures, which can be either commercially procured or developed in-house by the activity, must prevent, minimize, or assist the data processing environment to recover from any accidental or intentional , unauthorized modification, destruction, disclosure, or denial of service. This process of safeguarding data processing assets is called automatic data processing (ADP) security.

Perfect security is generally regarded as unattainable. Therefore, the objective of a good ADP security program is to reduce, for a reasonable cost, the probability of loss to an acceptable level and to provide adequate recovery in case of loss [Ref. 2: p. 2]. A good program can only be achieved by having top management ultimately responsible for the ADP security program and by applying quantitative techniques to determine how much protection is needed to reduce the risk of operating to an acceptable level.

There are many approaches to help top management determine the appropriate ADP security policy. The most endorsed approach uses risk management as the tool to develop and implement that policy. Risk management is a methodology for

analyzing an environment and determining the optimal set of countermeasures needed to provide sufficient protection for that environment.

The General Accounting Office (GAO) reports that "... risk management is an element of managerial science that is concerned with the identification, measurement, control, and minimization of impact of uncertain events upon organizations that depend upon automated operations" [Ref. 2: p.35]. Robert H. Courtney, Jr., a pioneer of risk analysis techniques, says:

> Most management decisions involve the assumption of risk--the chance that things may not turn out the way we hope or want them to. Decisions made in spite of uncertainties and, indeed, in recognition of them are generally accepted as essential to dynamic successful management. Most frequently, however, the key to success lies not in the willingness to accept uncertainty, or to assume risk, but in the ability to recognize and quantify the elements of that risk so as to deal with them in a fully objective way. [Ref. 3: p. 4]

B. REQUIREMENTS FOR RISK MANAGEMENT

1. Federal, Department of Defense and Department of the Navy

The first federal regulation that addressed data security and risk analysis was the Privacy Act of 1974. Two major concerns precipitated this law: the total amount of personal information maintained by Federal agencies, and the potential risk posed by the increasing use of computers and sophisticated information systems. The Act defines specific responsibilities to guarantee that personal information about individuals collected by Federal agencies is limited to that which is legally authorized and necessary and is maintained in a manner which precludes unwarranted

intrusions upon individual privacy. The Act requires each agency to establish appropriate administrative, technical, and physical safeguards to ensure the integrity and confidentiality of personal information and to protect against any anticipated threats or hazards which could result in harm, embarrassment, inconvenience, or unfairness. [Ref. 4: p. 133]

When the Act became law on 31 December 1974, virtually every agency in the Federal government was impacted. Because of its implementation responsibility, the Office of Management and Budget (OMB) was particularly affected. OMB responded to the Act by issuing OMB Circular No. A-108, "Responsibilities for the Maintenance of Records About Individuals by Federal Agencies," dated 1 July 1975. Specific taskings associated with this circular are:

- The National Bureau of Standards (NBS) is responsible for issuing standards and guidelines on computer and data security.
- The General Services Administration (GSA) is responsible for revising computer and telecommunications procurement policies to ensure compliance with applicable provisions of the Act.
- The (White House) Office of Telecommunications Policy is responsible for reviewing Federal agency policy on interconnection and operational control of networks and communication security devices. [Ref. 4: p. 19]

The Privacy Act of 1974 was the first in a series of events during the 1970's that focused national level attention on the value and vulnerability of Federal data processing. Following the Act, in the spring of 1976, three GAO reports were published that brought congressional attention to this growing concern and increased awareness of the potential risks facing the Federal ADP community. Shortly

thereafter, Senator Abraham Ribicoff directed the Committee on Government Operations to conduct a preliminary inquiry into the problems of computer security. The Committee subsequently issued two studies addressing the subject. The first report reviewed some of the major technological issues and problems identified by GAO and provided an extensive collection of articles written by experts in the field of computer security [Ref. 5]. The follow-up report recommended that OMB direct Federal agencies to put into effect appropriate computer security controls and safeguards, that NBS prepare physical and personnel standards for protecting Federal ADP systems according to their sensitivity, and that Federal agencies improve coordination of computer resource protection efforts [Ref. 6: p. 276].

In response to these Congressional recommendations, OMB issued Transmittal Memorandum No. 1 to Circular A-71 in July 1978 [Ref. 7]. In announcing this comprehensive Federal computer security program, OMB Director James T. McIntyre, Jr., said,

> Computer technology now impacts almost every facet of American life. The protection of the technology against unwarranted, unauthorized and illegal users is a major challenge. This program addresses that challenge in the Federal Community. [Ref. 8]

The Transmittal Memorandum requires each agency computer security program to satisfy the following requirements:

- Conduct a periodic risk analysis for each computer installation operated either in-house or commercially.
- Assign responsibility for security to a management official knowledgeable in data processing and security matters.

- Establish a management control process to ensure that appropriate administrative, technical, and physical safeguards are incorporated.
- Ensure that appropriate security requirements are included in specifications for the acquisition or operation of computer resources.
- Establish personnel security policies for screening all individuals participating in the design, operation, or maintenance of or having access to Federal computer systems.
- Conduct periodic audits or evaluations and recertify the adequacy of the security safeguards of each operational sensitive application.
- Ensure that appropriate contingency plans are developed, maintained, and tested to provide for continuity of operations should events disrupt normal operations. [Ref. 7: p. 3]

Also in 1978, Presidential Directive Number 24 was issued which transferred the functions of the White House Office of Telecommunications Policy to the Department of Defense (DOD) and Department of Commerce. DOD was tasked with telecommunications policy relating to national security. All other telecommunications policy functions were assigned to the National Telecommunications and Information Administration under the Department of Commerce.

Because DOD is the largest Federal agency in terms of personnel strength, budget size, and number of computers, it is the most affected by the Federal policies discussed above. DOD reacted to OMB Circular A-108 by publishing DOD Directive 5400.11 [Ref. 9]. This directive established a DOD Privacy Board with oversight review authority, and included guidelines for safeguarding personal data in ADP systems as an appendix. DOD approached Circular A-71

somewhat less decisively. Since DOD had been involved with the protection of classified data for years, it sought to apply the framework of A-71 to the existing classified arena and integrate the additional protection requirements for unclassified ADP systems. The objective of DOD was to develop an overall systematic concept to security that applied safeguards to each ADP system commensurate with the sensitivity of the data being processed. DOD forwarded the approach to OMB in a memorandum dated 30 January 1980 and appropriately entitled "A Comprehensive Information Security Program." By the issuance of this memorandum, all military departments were tasked to establish formal risk management and computer security programs as delineated in Ref. 7.

In reaction to the proposed comprehensive DOD ADP Security Program, the Department of the Navy (DON) promulgated OPNAVINST 5239.1, which assigned specific ADP security responsibilities within the Navy and established Designated Approving Authorities (DAA). The current version of this instruction [Ref. 10] directs each Navy activity to assign ADP security responsibilities, establish an Activity ADP Security Program, implement a formal Risk Management Program, and be accredited by the appropriate DAA.

OPNAVINST 5239.1A, together with the Naval Material Command (NAVMAT) and the Naval Supply Systems Command (NAVSUP) implementations, should after a period of time substantially increase the protection afforded to DON ADP systems. The requirements for a Risk Management Program are summarized in Table I, which lists the regulations and reports published in the last decade.

2. Operational Requirements

In order to establish and manage an Activity ADP Security Program, it is encumbent on activity top management (Commander, Commanding Officer, Officer in Charge, or

TABLE I

Federal/DOD/DON Regulations on ADP Security

1974 - Privacy Act of 1974 (Public Law 93-579)

1975 - OMB Circular No. A-108, "Responsibilities for the Maintenance of Records about Individuals by Federal Agencies," 1 July 1975

- DODD 5400.11, "Personal Privacy and Rights of Individuals Regarding their Personal Records," 4 August 1975

- NAVMATINST 5211.2, "Personal Privacy Act and Rights of Individuals Regarding their Personal Records," 26 September 1975

- NAVSUPINST 5211.1, "Personal Privacy Act and Rights of Individuals Regarding their Personal Records (Privacy Act of 1974, Public Law 93-579)," 18 November 1975

1976 - GAO Report, "Improvement Needed in Managing Automated Decisionmaking by Computers Throughout the Federal Government," April 1976

- GAO Report, "Computer-Related Crimes in Federal Programs," April 1976

- GAO Report, "Managers Need to Provide Better Protection for Federal Automatic Data Processing Facilities," May 1976

- Senate Committee on Government Operations, "Computer Abuses - Problems Associated with Computer Technology in Federal Programs and Private Industry," June 1976

1977 - Senate Committee on Government Operations, "Computer Security in Federal Programs," February 1977

- NAVMATINST 5510.17, "Security of ADP Systems," 22 March 1977

1978 - OMB Circular No. A-71, Transmittal Memorandum No. 1, "Security of Federal Automated Information Systems," 27 July 1978

1979 - SECNAVINST 5211.1C, "Personal Privacy and Rights of Individuals Pertaining to Their Personal Records," 4 December 1981

1980 - DOD Memorandum, "A Comprehensive Information Security Program," 30 January 1980

- NAVSUPINST 5510.6A, "Security Requirements for ADP Systems," 28 May 1980

1982 - OPNAVINST 5239.1A, "Department of the Navy Automatic Data Processing Security Program," 3 August 1982

Director) to implement a Risk Management Program. In the process of formalizing this program, top management must establish ADP security policy with explicit regard to OPNAVINST 5239.1A and the unique requirements and constraints of the activity ADP systems. [Ref. 10: p. 1-2]

Since activities have invested heavily in computer resources, they often desire to maximize the utilization of their resources by sharing them among users, both internal and external to the activity. Each user has a different need-to-know and need-to-utilize criteria for accessing his information. This requires that individual user data integrity be assured, while concurrently providing shared access to the ADP system. For example, an ADP activity might furnish services to both fiscal and logistic users, each of which expects its assets to be protected and available upon demand. The task of simultaneously sharing and protecting an ADP system is the responsibility of the activity providing automated support.

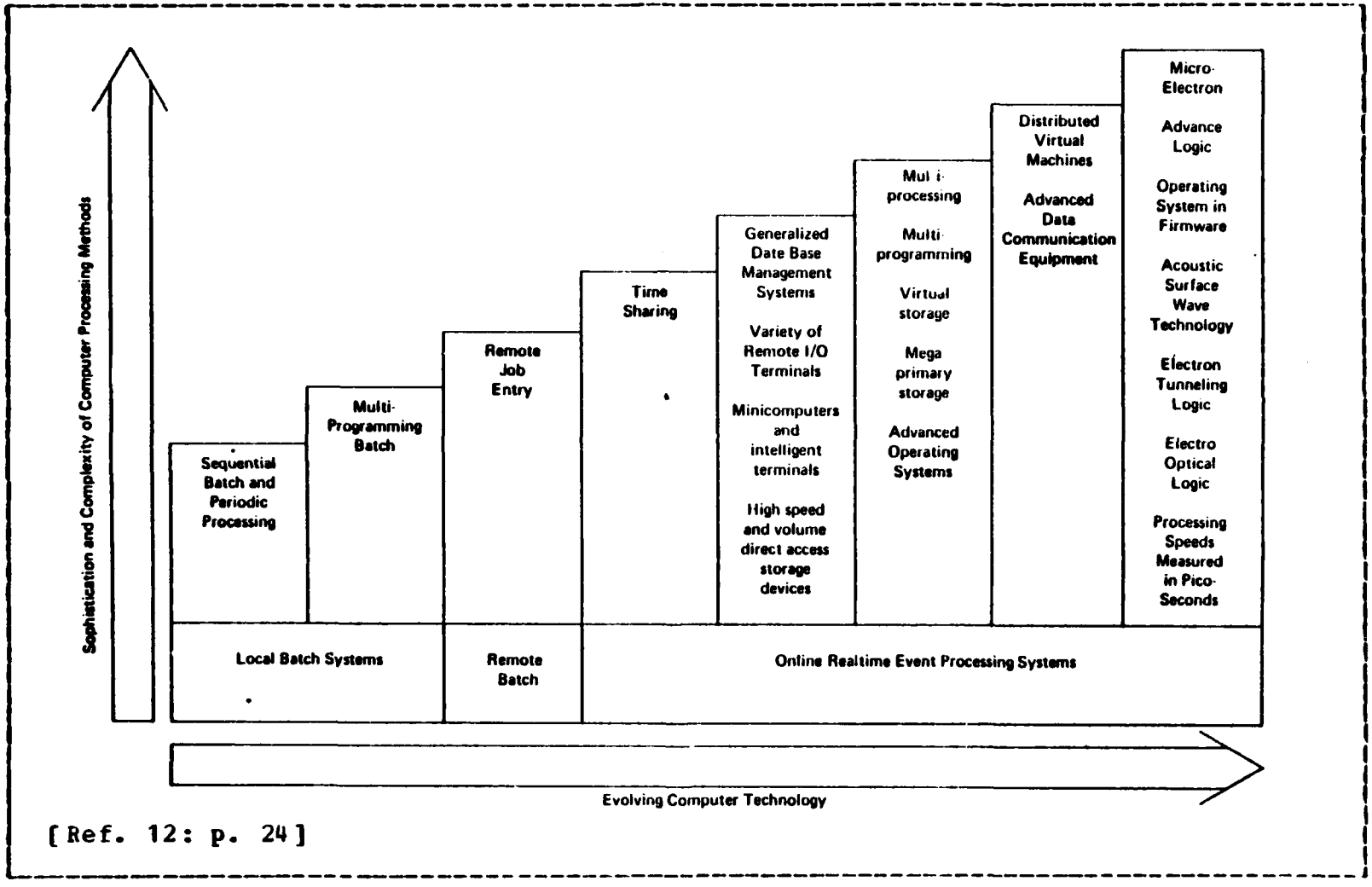
Ref. 10 requires that each Navy ADP activity be accredited for operational use. By accrediting an activity, the DAA, which in some cases is the activity Commanding Officer, acknowledges that the risk of operating the data processing environment is acceptable, in light of the activity's mission and the users' dependence on automated support, and approves the system for operational use. To obtain accreditation, top management must quantify the operational risk and implement an Activity ADP Security Plan. The Risk Management Program described in Ref. 10 and further explained by this thesis is the tool used by top mangement to quantify the risk present, evaluate the cost-effectiveness of proposed countermeasures, and provide for recurring review of the activity's ADP security posture.

C. INTRODUCTION TO SPLICE

The Stock Point Logistics Integrated Communications Environment (SPLICE) is a NAVSUP Project designed to integrate all interactive processing and telecommunications required by current and projected applications systems operating within the Uniform Automated Data Processing System for Stock Points (UADPS/SP). The SPLICE Project will use standard minicomputers and modular software components. A "foreground/background" concept will be implemented with SPLICE minicomputers, which will serve as a front-end-processor for the existing stock points medium sized Burroughs systems. [Ref. 11: p. 1]

More than twenty new applications systems under development and the current UADPS/SP system comprise the "SPLICE Umbrella." These systems will require considerable interactive and telecommunications support at more than fifty UADPS/SP activities. SPLICE will provide a responsive and economical support capability without saturating the current Burroughs mainframes, and will simplify the eventual mainframe replacement [Ref. 11: p. 1]. SPLICE will present a user oriented environment which will provide many standard operating functions such as terminal management, communications management, database management, and peripheral management. Additionally, there will be many support functions such as standard software tools (compilers, etc.), recovery management, and security. The existing Burroughs mainframes will provide large file processing functions and report generation.

As seen in Figure 1.1, the evolution of computer technology has resulted in the design and implementation of very complex and sophisticated automated environments. The risk of operating these new environments is directly proportional to their overall complexity. As a point of reference, the operational SPLICE Network will fall at the very high end of



[Ref. 12: p. 24]

Figure 1.1 Technology versus Complexity.

the technology and complexity scales. The Navy's increased operational dependencies on automated systems demand that the risk in SPLICE be evaluated and managed at an acceptable level.

D. OBJECTIVES OF RESEARCH

Research by Naval Postgraduate School faculty and students on the SPLICE Project is concerned with systems analysis and preliminary design proposals for many of the functional areas of SPLICE. This thesis defines a Risk Management Program to evaluate and manage the risk associated with the operation of SPLICE. The methodology proposed draws upon current government and industry techniques and conforms to existing DON and NAVSUP guidance.

Ref. 11 tasked NAVSUP 0415 and the Fleet Material Support Office (FMSO) 94 with conducting a risk analysis of the SPLICE system. It is intended that the Risk Management Program proposed in this thesis be used as a tool to quantify the risk in SPLICE. Together with information about and simulation of the eventual operational SPLICE activities, this tool can be used to identify those initial design specifications needed to reduce the risk in SPLICE.

E. LIMITATIONS AND ASSUMPTIONS

1. Defense Data Network

The original SPLICE specifications required the Network Interface Subsystem to provide access to the AUTODIN II Network [Ref. 13: p. 57]. On 2 April 1982 Deputy Secretary of Defense Carlucci directed the termination of the AUTODIN II program and the immediate development of the Defense Data Network (DDN) [Ref. 14]. It is current DOD policy that all data communications users will be integrated into the DDN.

It is assumed that the SPLICE Network will comprise a "community of interest" within the DDN. A brief description of the DDN and a summary of the security features provided by the DDN is included as Appendix C.

2. Level II Data

It is assumed that the data processed within the SPLICE Network is Level II data, which is defined in Ref. 10 as unclassified data requiring special protection. Since the SPLICE application systems will be processing financial and other management data which is by definition "Sensitive Business Data," it requires protection for reasons other than being classified or personal data. It is judged that the potential impact of modification or destruction of the data is severe enough to justify a greater degree of protection than required for other unclassified information.

3. Activity ADP Security Plan

The majority of SPLICE configurations will be located at Navy ADP activities, which are subject to the Department of the Navy ADP Security Program [Ref. 10: p. 3]. Although the proposals set forth in this thesis follow the guidance of Ref. 10, they are concerned only with the risk management of the SPLICE configuration(s) and will not constitute an Activity ADP Security Plan. The Activity ADP Security Plan must be much more comprehensive in order to implement the overall Activity ADP Security Program. In particular, Appendix J of Ref. 10 outlines the mandatory minimum requirements for DON ADP activities. Additional minimum security requirements for SPLICE are given in Refs. 11 and 15.

4. Applications Software Security

Each applications software system must provide its own unique internal security and data integrity, adhering to activity software development policy. Examples of such applications software integrity considerations are computations of money figures (such as what to do with remaining fractions of cents, if any) and maintenance of application-unique audit trails (such as the Transaction Reconstruction File in UADPS/SP). At a minimum, applications software must incorporate security and audit controls listed in Appendix I of Ref. 10. Applications processing financial data should adhere to NAVCOMPTINST 7000.36, Financial Management Systems; Standard criteria for ADP internal control of.

II. OVERVIEW OF RISK MANAGEMENT

A. RISK MANAGEMENT TERMINOLOGY

Before proceeding with a discussion of the functional phases of risk management, it is essential that the terms risk, threat, vulnerability, and countermeasure be explained.

1. Risk

In Webster's Collegiate Dictionary, risk is defined as the possibility of loss or injury; a dangerous element; or the degree of probability of a loss. Unfortunately, the term risk is not a universally defined term. Risk is perceived differently, depending on the circumstance or community.

The insurance industry uses the idea of an "insurable risk." A company identifies both the known and uncertain elements of operating a business and minimizes their potential loss by buying insurance. The insuring agent, using empirical and statistical data, sells protection to the company in the form of financial compensation should its assets be lost. To determine how much risk is involved, the agent relies on historical data, prediction models, and business experience. Unfortunately, the computer industry is relatively new and little analytical data is available for assessing the areas and extent of potential security risks.

In business economics, there are two types of risk: speculative and pure. When a business invests, and there is a degree of uncertainty as to whether that investment will result in a gain, the risk is speculative. If the only

possible outcome is either loss or no change, the risk is classified as pure.

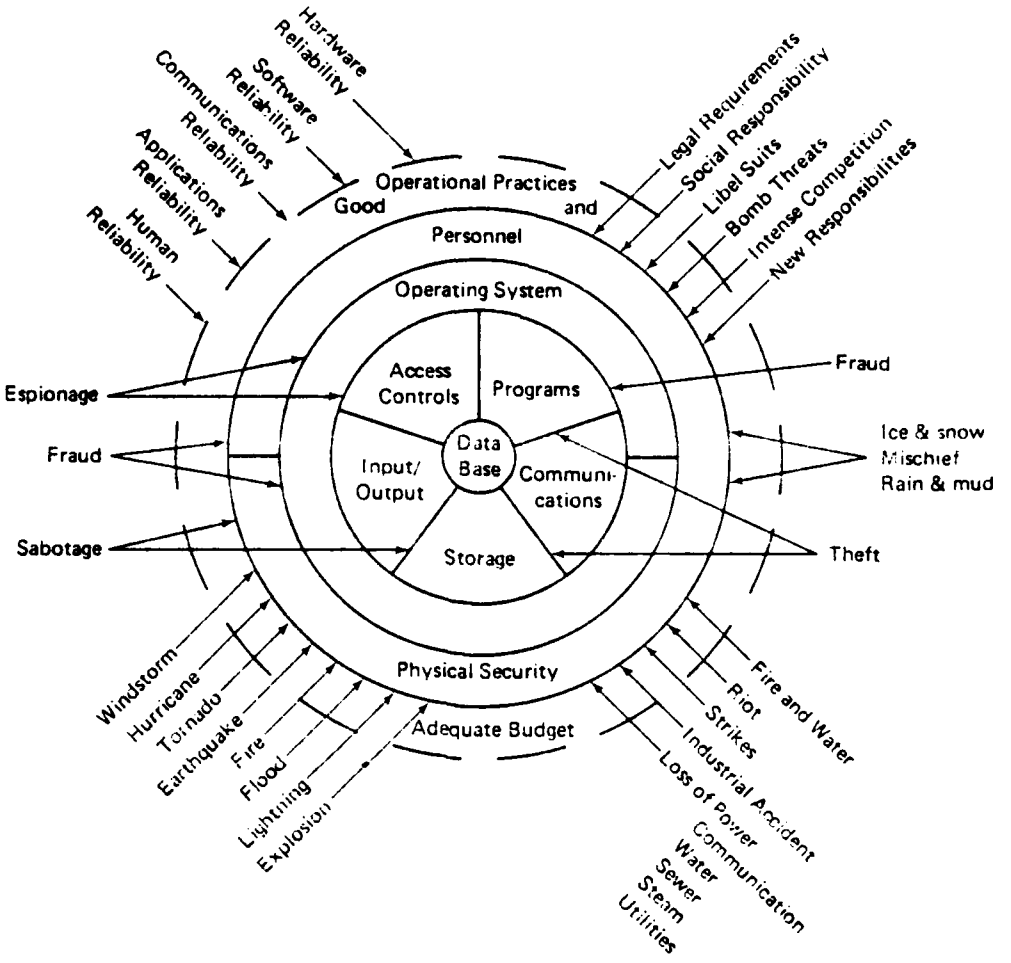
In the context of ADP security, only a pure risk can exist. Risk within the data processing community is defined as the likelihood of a loss and the expected amount of that loss with respect to the assets of an activity.

2. Threat

H. Stephen Morse of the System Development Corporation defines a threat as any action, event, or circumstance, the occurrence of which is likely to adversely affect the assets of an activity. Threats exist in general because of the unpredictability of the real world and people. The presence of a threat does not equate to harm or loss. For that to happen, there must be a successful attack by a threat agent using a specific technique, methodolgy, or spontaneous occurrence.

Threat agents are classified as natural environmental factors (tornado, flood, fire, etc.), authorized users (programmers, operators, etc.), or hostile agents (anyone not an authorized user). A threat agent causes a threat to be realized by attacking the assets. The attack can impact these assets in at most four areas: modification, destruction, disclosure, or denial of service. Whether the attack renders harm or loss to the activity is dependent upon the threat agent successfully penetrating the existing countermeasures and exploiting weaknesses (vulnerabilities) in the data processing environment.

The threats facing an activity can be a function of its geographic location, personnel workforce, processing mode, physical facilities, or computer system configuration. Since these elements are constantly changing, threats are considered dynamic and should be continually monitored.



[Ref. 16: p. 174]

Figure 2.1 Some Typical Threats and Their Usual Defense.

Perhaps the easiest way to understand threat is by an example. Although the existence of threats is beyond our control, a threat will not necessarily materialize or cause harm. There is always the threat of a fire, but that does not mean there will be a fire. The occurence of a fire and the extent of damage a fire would cause depends in part on

the weaknesses in the facility. The weakness, in this case, is the lack of fire prevention measures. Figure 2.1 shows some typical threats and their usual defense.

3. Vulnerability

OPNAVINST 5239.1A defines a vulnerability of a computer system as a weakness in its physical layout, organization, procedures, hardware, or software that may be exploited to inflict harm. As with a threat, the presence of vulnerability does not in itself cause harm; a vulnerability is merely the condition or set of circumstances of which the threat agent can take advantage to inflict damage. [Ref. 10: p. A-17]

The vulnerabilities of a computer system increase directly with its complexity; remotely accessed resource-sharing computer systems that allow remote job entry are significantly more likely to have weaknesses than a dedicated, batch-processing, stand-alone system with no remotely located terminals. Figure 2.2 illustrates some potential vulnerabilities of a computer system.

One purpose of evaluating a data processing environment is to identify all vulnerabilities existing in the facility, system, or operation. By conducting a thorough analysis of identified weaknesses and weighing each of the probabilities of a successful attack by a threat agent, the vulnerabilities of the data processing environment can be measured. Vulnerabilities, unlike threats, are generally under the control or influence of the data processing management, and can be modified to reduce the severity of an attack.

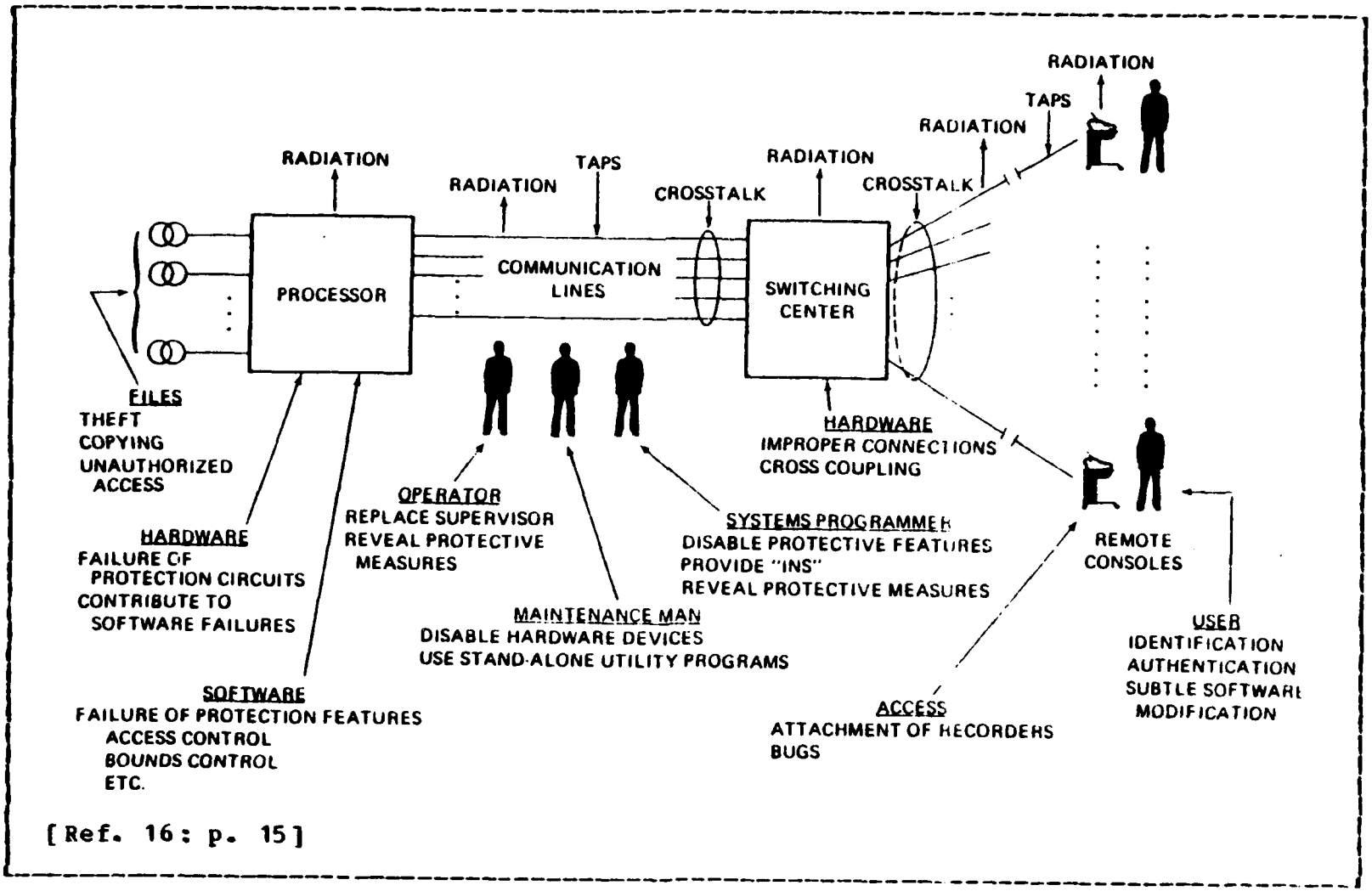


Figure 2.2 Potential Computer System Vulnerabilities.

4. Countermeasure

The words countermeasures, safeguards, protective or backup measures, and control mechanisms are often viewed as being synonymous. A countermeasure is any protective action, device, procedure, technique, or mechanism that when implemented reduces the activity's vulnerability to successful attacks. These corrective features are designed and developed to protect the assets of an activity. The purpose of a countermeasure is to either reduce the probability of a successful attack or minimize the impact of an attack. Countermeasures are therefore technical or managerial mechanisms for controlling the risk to which an activity is exposed. Some examples are contingency plans, backup copies of software, access control procedures, and audit trails.

As shown by Figure 2.3, risk management is concerned with the interaction among the terms just defined. Risk is the extent and probability of loss due to the manifestations of threats (attacks) at points of vulnerability in light of installed countermeasures.

B. RISK MANAGEMENT: A FUNCTIONAL APPROACH

Risk management with respect to computers is a new discipline that provides quantifiable techniques for assessing the risk of operating a computer system in light of existing protection measures, and determining the requirement for additional countermeasures to protect that system. Leading authorities in the data processing industry are using various techniques for analyzing risks. However, most agree on a formal, four-phased approach to risk management: risk analysis, management decision, risk control, and operational continuity.

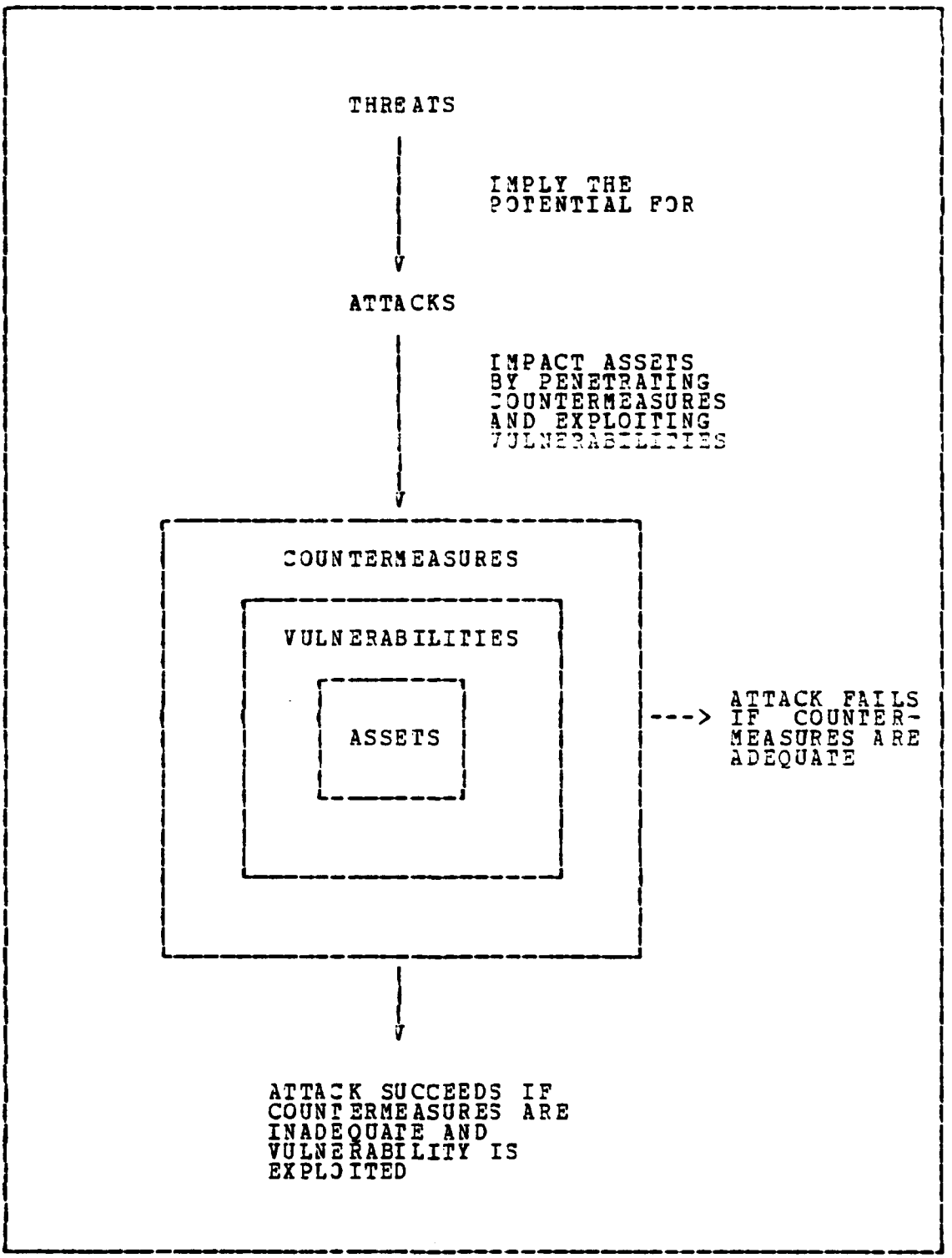


Figure 2.3 Factors of Risk Management.

For a risk management program to effectively enforce the ADP security policies and control the ADP security posture of an activity, a total commitment is needed from top management. High level attention will improve the cooperation across interdepartmental lines and will foster an increased security awareness. Top management commits itself to a risk management program by making resource allocations in terms of both skilled manpower and budgetary allotments and by integrating security objectives into the existing managerial responsibilities at all levels.

Top management is also responsible for promulgating policy on the frequency and conditions for initiating the risk analysis phase. According to Ref. 10, a risk analysis will be conducted at least every five years, or whenever in the judgement of top management a system configuration or facility change has been effected that warrants a requantification of the risk.

1. Risk Analysis

The quantification of risk is not new. As early as the seventeeth and eighteenth centuries, noted men such as Pascal, Bernoulli, and Bayes applied risk analysis techniques to "games of chance." Risk analysis has recently been applied to the data processing environment, expanding the "game of chance" from computing the odds for a win to quantifying the probability of loss or harm for a computer system.

The purpose of conducting a risk analysis of a data processing environment is to quantify the damage and operational impact resulting from the successful attack by a threat agent and the likelihood of such an attack occurring [Ref. 17: p. 8]. The analysis produces an annual loss expectancy (ALE) value, which is a quantitative estimate of the potential average yearly financial loss resulting from

any accidental or intentional unauthorized modification, destruction, disclosure, or denial of service. This ALE value is a baseline for assessing the ADP security posture of an activity.

As shown by Figure 1.1, the risk an activity faces is directly proportional to the complexity of its data processing environment. Because of this, top management bases the scope and depth of the risk analysis on the complexity of the particular environment being evaluated. Some factors that are pertinent to the decision are the value of the physical facility, the value of the data (both internally to the activity and externally to others), the configuration of the ADP system, and the criticality of the data processing service to the activity's and users' missions.

The risk analysis technique attempts to predict future risk exposure of an activity based on a thorough evaluation of its assets, threats, vulnerabilities, and existing countermeasures. This evaluation relies heavily on the professional experience and technical knowledge of the risk analysis team. For this reason, it is vital that the team be drawn from both the data processing department and the users' departments in order to take advantage of their diverse backgrounds and technical expertise. The team members should be highly skilled professionals, whose selection will substantially influence the quality of the final risk analysis product. Additionally, the risk analysis team must be supported at all levels if the analysis is to accurately reflect the security posture of the activity.

2. Management Decision

In this phase top management decides, based on the risk analysis, the activity's mission, and the users' degree of dependence on automation, if the existing countermeasures

provide sufficient protection. Before making this decision, top management reviews the risk analysis to determine if appropriate assumptions were made and operational constraints were considered. The risk analysis quantified the "current level" of risk associated with operating the existing computer system and documented the activity's ADP security posture. The risk analysis should be presented to top management in such a manner that decisions can be made in relation to the documented threats, vulnerabilities, and countermeasures.

At this junction, the Risk Management Program can follow one of two directions, contingent on the decision of top management. If top management judges the current level of risk as acceptable, then the Operational Continuity Phase is entered. By progressing directly to that phase, top management is explicitly acknowledging that existing control practices and procedures are sufficient and the current security level is to be maintained. On the other hand, if top management decides that the current level of risk is unacceptable, then the Risk Control Phase is initiated. This means that top management is not willing to tolerate the risk. Before the Risk Control Phase is begun, top management should assign a risk control team and provide guidance abouts those deficiencies of greatest concern. The risk control team should be composed of a greater proportion of data processing technicians than the risk analysis team.

3. Risk Control

The function of this phase is to propose to top management an optimal set of countermeasures that have proven cost-effective and technically feasible. The countermeasures needed to bring the risk of operating to an acceptable level are selected from a combination of risk avoidance and reduction techniques.

Within the data processing environment, a risk is avoided by determining that a particular ADP specification should be abandoned, redesigned, or deferred because the potential harm is too great to be controlled with existing technology. Countermeasures to reduce risk fall into three basic categories:

- Protective measures which reduce the damaging effects of external events.
- Control measures which reduce the likelihood of undetected errors or fraudulent modifications and unauthorized disclosure.
- Back-up (contingency) measures which provide alternative means for carrying on the mission of an activity subsequent to an event which disrupts normal operations. [Ref. 18: p. 224]

After top management selects and approves those measures that have the greatest potential of minimizing the overall losses, the risk control team prioritizes them for implementation. This phase is complete when top management accepts the set of proposed additional countermeasures and approves their implementation plan.

4. Operational Continuity

The Operational Continuity Phase is initiated either after completion of the Risk Control Phase or immediately following the Management Decision Phase. If the Risk Control Phase was executed, resources are dedicated in this phase to carrying out the action plan developed for implementing the approved additional countermeasures.

During this phase, the DAA makes the technical and managerial policy decision regarding the accreditation of the activity. That decision is made immediately if no Risk Control Phase was executed, or after the implementation of

additional countermeasures. Regardless of whether or not additional countermeasures are being implemented, the process of risk management continues. This ongoing effort is considered essential to preserving the ADP security posture of the activity and includes continual review, audit, and evaluation of the data processing environment. This phase is terminated when it is deemed necessary to reinitiate the Risk Analysis Phase because either a five year time interval has passed or the policy of top management so dictates.

III. RISK MANAGEMENT PROGRAM

The proposed Risk Management Program furnishes a framework which is tailored to the unique aspects of the data processing environment. The foundation of this program is taken from Refs. 2 and 10 and the recent experiences of industry. Quantitative techniques are used in the Risk Analysis and Risk Control Phases. These techniques do not utilize exact values; instead, values are scaled by orders of magnitude. The use of relative magnitude is to accomodate the lack of empirical data, incomplete knowledge on the future likelihood of attacks, and inconclusive proof of the effectiveness of countermeasures.

As a first step in establishing a formal Risk Management Program, it is recommended that activity top management implement a managerial structure which includes an ADP Security Staff as described in Ref. 10. The activity is directed to the Commander, Naval Data Automation Command (COMNAVDAC) for technical assistance in conducting a risk analysis. Within the DON, COMNAVDAC is responsible for providing assistance as requested and with ensuring that risk management expertise is shared across activity boundaries.

This chapter is broken into the phases of a Risk Management Program and is intended to meet two objectives. The first is to describe in a cohesive manner the philosophy of each phase. The second is to give, where necessary, specific implementation considerations independent of the philosophy.

A. RISK ANALYSIS

According to Ref. 10, there are three distinct steps in a risk analysis. These steps, as shown in Figure 3.1, must

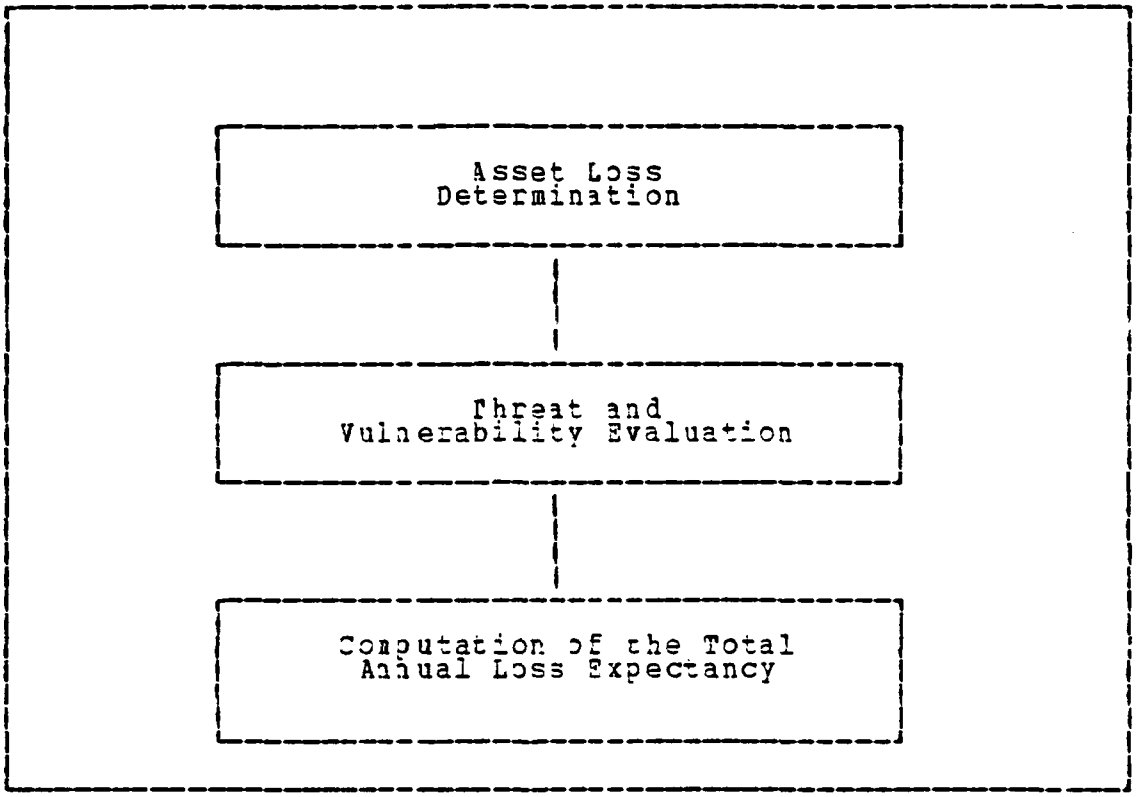


Figure 3.1 The Major Steps of Risk Analysis.

be completed in sequential order. The purpose of the Risk Analysis Phase is to quantify in accordance with the policy guidelines from top management the risks of a specific data processing environment in relation to its threats, vulnerabilities, and existing countermeasures. The following conceptual model and implementation considerations elaborate on how this quantification is performed.

1. Model

The risk analysis model is an abstraction of the risk analysis process presented in Appendix E of Ref. 10. It takes into account the work of Robert H. Courtney [Ref. 3], NBS [Ref. 17], and Jerry Fitzgerald [Ref. 19]. The model allows one to systematically quantify asset losses and attack frequencies on an annualized basis and to calculate from these the total annual loss expectancy (ALE) of an activity.

a. Asset Loss Determination

This step identifies all of the assets within an activity and quantifies the activity's loss should they be harmed. The degree to which assets should be separately identified is addressed in the implementation considerations. In addition to naming an asset, a textual description is written to document how that named asset could be impacted by threats in general. Next, for each named asset, four loss values are determined, one for each threat impact area. The four threat impact areas are modification, destruction, disclosure, and denial of service. Each loss value is an estimation in dollars of what an activity will lose if one attack is completely successful in causing harm in that impact area to the asset. Put another way, given that there is a one hundred percent probability of one successful attack, how much is an activity willing to pay to prevent that attack? This step is completed by transforming each loss determination into a loss rating [Ref. 17: p. 10]. The model component representing this step is summarized in Table II.

TABLE II

Asset Loss Determination Model

The loss determination function, L(i,A), is an empirical estimation of loss, in dollars, of asset A in impact area i, rounded to the nearest exponential value of ten.

The function is expressed as:

L(i,A) = function [D(A), N(A)], rounded

Where:

i = the threat impact area (modification, destruction, disclosure, or denial of service)

A = the unique name of an asset

D(A) = the description of how asset A could be affected by threats

N(A) = the number of identical assets A subject to the same threats

The loss rating function is a logarithmic mapping from L(i,A) onto an ordinal integer scale ranging from 0 to 8. The zero rating indicates asset A is not affected in a particular impact area i.

The function is expressed as:

$$LOSS(i,A) = \log_{10}[L(i,A)]$$

b. Threat and Vulnerability Evaluation

This step identifies each threat which could possibly affect the assets of an activity, provides pertinent textual descriptions, and expresses the probability of an attack with an annualized frequency rating. The first description defines the threat and enumerates specific threat agents. The second description discusses the vulnerabilities which are susceptible to attacks by threat agents. The last description describes existing countermeasures

installed to counter those attacks. Examples of threats common to the current minicomputer environment are identified in the implementation considerations.

Since the realization of a threat can have an impact assets in four areas, four frequency occurrences must be estimated. The frequency occurrence represents, on an annualized basis, how often a threat agent can be expected to penetrate the defenses of an activity and successfully attack assets. This step concludes by transforming the frequency occurrence for each impact area into a frequency of successful attack rating [Ref. 17: p. 10]. The model component for this step is summarized in Table III.

c. Computation of the Total Annual Loss Expectancy (ALE)

The final step of the risk analysis calculates the activity's Total ALE by a series of computations. The Total ALE quantifies the average yearly risk exposure in dollars resulting from modification, destruction, disclosure, or denial of service. The activity's risk exposure reveals the degree to which the existing vulnerabilities permit threats to be realized against the assets of the data processing environment. The first computation uses a matrix of all assets and threats for each impact area. An ale (uncapitalized) is computed for each combination of loss rating (of a single asset) and frequency of successful attack rating (of a single threat) paired by the same impact area [Ref. 17: p. 10]. This ale is the risk exposure for that specific asset and threat intersection. The second computation computes the ALE for impact area i as the sum of all ale's in impact area i. The last computation totals the four impact area ALEs. The model component for this last step is presented in Table IV.

TABLE III

Threat and Vulnerability Evaluation Model

The frequency occurrence function, F(i,T), is a stochastic estimate of the frequency per year of successful attack by threat T in impact area i.

The function is expressed as:

F(i,T) = function [D(T), V(T), C(T)]

Where:

i = the threat impact area (modification, destruction, disclosure, or denial of service)

T = the uniquely named threat

D(T) = the definition of threat T and listing of of specific threat agents

V(T) = the discussion of the vulnerabilities which allow threat T to materialize

C(T) = the description of the existing countermeasures to counter threat T

The frequency of successful attack rating is a mathematical mapping from F(i,T) onto an ordinal integer scale ranging from 0 to 8. The zero rating indicates that threat T does not affect any of the activity's assets in a particular impact area i. After the rating is computed, it is rounded to the nearest integer.
The function is expressed as:

$$ATTACK(i,T) = \log_{10}[3000 \times F(i,T)], \text{ rounded}$$

2. Implementation Considerations

Top management begins this phase by selecting the risk analysis team and providing them policy guidance on the scope and depth of the risk analysis. The members are assigned in writing and their accompanying duties and responsibilities are documented. Team selection is based not only on individual diversity of specialized technical

TABLE IV

Activity Total ALE Computation

The individual "ale" function is a mathematical mapping from LOSS(i,A) and ATTACK(i,T) onto the the annual loss expectancy, in dollars, associated with each combination of asset A and threat T, having the same impact area i.
The function is expressed as:

$$ale(i,A,T) = 1/3 * 10^{[LOSS(i,A) + ATTACK(i,T) - 3]}$$

The ALE function by impact area i is a summation of the "ale"s computed above and is expressed as:

$$ALE(i) = \sum_{\forall A} \left[\sum_{\forall T} ale(i,A,T) \right]$$

The activity Total ALE function is a total of the four impact area ALEs and is expressed as:

$$\text{Activity Total ALE} = \sum_{\forall i} ALE(i)$$

talents, but also on familarity with the activity's mission and knowledge of the data processing services provided.

The scope and depth of the risk analysis depends on the complexity of the data processing environment. The SPLICE Network, as previously described in Section I.C., will be a decentralized, interactive, telecommunications environment. Risk increases in direct proportion to the complexity of the data processing environment. The SPLICE falls on the high end of the complexity scale as seen if

Figure 1.1. It is because of this potentially large risk exposure that the policy guidance concerning the risk analysis should at the least address the following.

The risk analysis conducted during the developmental phase of SPLICE will be different from the analysis conducted after the system is operational. The risk in the developmental phase is quantified either by simulating the operational environment or by comparing the eventual operation to one already in existence. The analysis of the developmental phase deals with educated estimates and design time considerations, while the analysis of the operational system deals with concrete data and mission-essential requirements. Since a risk analysis is required early in a system's life cycle, hardware and software countermeasures can be included in the final specifications and implemented at a reasonable cost. If the risk is not evaluated until the operational stage, many technically feasible countermeasures are no longer practicable and less effective control measures are used to manage the risk.

As stated earlier, a risk analysis is reinitiated either after five years or whenever the data processing environment has been affected by a significant change. Due to this recurring cycle, policy guidance is needed on the applicability of a previous risk analysis. Most of industry agrees that if five years has passed, then the risk should be thoroughly reexamined and documented. On the other hand, if only one area has realized a major change and less than five years has passed, then only that portion of the environment should be reevaluated. During the reevaluation, the risk analysis team is cautioned not to overlook those areas indirectly impacted by the change.

The final area requiring policy guidance concerns the level of detail required to document the estimated loss expectancies and frequency occurrences. The degree of

granularity imposed by top management directly correlates to the time and resources required to conduct an activity risk analysis. The level of detail should be sufficient enough for the risk analysis to be judged credible and defensible.

Having discussed the policy areas requiring the attention of top management, it is now time to focus on the practical considerations of actually conducting a risk analysis. The guidelines provided in the next two sections are general rules of thumb synopsized from Refs. 10, 33, 20, and 21. Ref. 10, Appendix E contains the forms required by the DON for documenting an activity's risk analysis.

a. Asset Identification and Loss Expectancy

Assets which function as a single unit or application are identified as a whole asset, since all of its components must be working for the asset to be serviceable. Likewise, if any component is damaged, the entire asset should be equally as likely to suffer the same damage as the component. Asset identification proceeds by reviewing the broad resource categories listed in Table V and by adding additional assets that are unique to the activity. The current DON guidance states:

> For each asset defined, all components of this asset should be in the same physical area, protected in the same manner, and subject to damage by the same threats. For example, consider six identical computers as six separate assets because damage to one of them would not imply damage to all of them. On the other hand, do not treat a single computer as a collection of subparts because if one of these components were to fail, the entire computer would be damaged to a similar level. [Ref. 10: p. E-2]

The level of disaggregation and the method for determining the loss associated with each asset are two areas which must be standardized to minimize individual interpretations and double counting of losses. Some general

TABLE V

Asset Examples Identified by Resource Category

The Seven Categories of Assets

Categories	Representative Sampling
Information	System (audit trails, bootstrap files, performance statistics), application (master files, transaction data, output files), and backup copies
Hardware	Central processing system, storage media (disk packs, tapes, cards), special interface equipment (front-end-processors, database machines), and I/O devices (printer, terminals, disk drives)
Software	System (operating system, compilers, audit routines), application programs, and backup copies
Communication	Telephone circuits, communication processors, modems, and multiplexors
Personnel	Computer (operators, programmers), building (janitors, guards), support (auditors, secretarial, management, librarian), maintenance, and users
Administrative	Documentation, operational procedures, user guides, I/O procedures and records
Physical	Environmental Systems, buildings, office equipment, supplies and auxiliary power

guidelines on the appropriate level of disaggregation that can serve as standards are as follows.

- All information required to perform a single function should be grouped accordingly at that functional level. This is because only partial information is not sufficient for performing the application. For example, the master and transaction files of a payroll system must both be available to issue paychecks. This same reasoning applies to the other soft asset categories of

software and administrative documents and procedures. An operating system has many components such as a job scheduler, main memory manager, I/O supervisor, and others, which must all be operable to perform the task of managing the overall system. To consider each component as a separate asset would be incorrect because they all act as a single unit.

- The unique identification of fixed assets is somewhat easier as their physical boundaries are visually recognizable. Fixed assets include the categories of hardware, communication, and physical assets of an activity, and are usually controlled by serial numbers and custody cards. As with soft assets, fixed assets are grouped according to whether they act as a single unit. For example, the operator console of a computer system must be functioning, otherwise the computer system is inoperable. On the other hand, if one tape drive in an inventory of six starts to malfunction, only that tape drive is affected, not all of them.
- For the remaining asset category of personnel, no universal grouping method exists. Each activity must decide based upon their particular situation which grouping alternative is best. Some potential alternatives are by skills, experience, salary, department assigned, or job classification.

Determining the loss of an asset requires careful attention to how essential it is in supporting the mission and how much an activity will lose if it is damaged. The user expresses how essential an asset is by assigning it a criticality value that reflects the importance given to the utilization of that asset. As expected, it is not an easy decision, and once made should be reviewed and approved by all levels of management relying on that asset.

For fixed assets, the loss value for modification and destruction damage is determined by the repair cost, original cost, or replacement cost. Additionally for destruction, the loss value includes the cost of doing without that asset. For disclosure damage, the user quantifies the loss by determining the worth of the asset to someone else, such as a hostile agent (any unauthorized user). The remaining area of denial of service is much harder to quantify. One must envision a typical timeframe during which the asset would be unavailable to satisfy the user's demand for processing and estimate the maximum time period that is tolerable for the user to be without the service of that asset. Then, using these two timeframes, one determines the estimated cost of getting that service from a commerical timesharing company, realizing that the user with the shortest tolerable time period has the most critical need for service.

The soft assets of information, software, and administrative documents and procedures are subject to the same four areas of damage (modification, destruction, disclosure, and denial of service) as fixed assets. However, in determining their loss values for modification and destruction, a different approach is taken. Some soft assets of an activity are generated by an internal project team or created uniquely for a particular function of the activity. This means that if such an asset is destroyed, the loss value is estimated by the cost of recreating the asset and of doing without it. For modification damage, the loss value is determined by either revalidating all the files or recertifying the administrative documents and procedures. To quantify the damage resulting from disclosure or denial of service, the guidelines given for fixed assets are appropriate.

The issue of quantifying the loss value of assets for which there are replacement spares or duplicate copies needs clarification. If a terminal is destroyed for which there is a spare, then the loss due to destruction is only the terminal's replacement and installation cost and does not include the cost of not having the service available. If no spare is available, then the loss from destruction includes all three costs. Likewise, some soft assets, such as centrally designed software or off-the-shelf documentation, are easily replaced from another activity or commerical vendor. For example, if an application system for which there is a duplicate copy is modified or destroyed, then the loss value only includes the overhead and computer running time needed to install the backup. The point is that the loss value of assets for which there are replacements must only reflect the cost to install the backup and replace it. That cost might include the additional costs to bring the backup version into operational use.

When quantifying the loss value of personnel, one takes into consideration the availability of qualified personnel, whether unique training or knowledge is required, and the activity's ability to absorb the loss based on the current number of skilled personnel.

In summary, the importance of this step cannot be overemphasized since the data collected dramatically affects the analysis. The implementation considerations presented should be viewed as a baseline for the risk analysis team. Many additional constraints and guidelines are unique to each particular activity and must be identified and documented.

b. Threat and Vulnerability Evaluation

In the previous section, guidance was given on quantifying the loss expectancy of assets. This section addresses the opposite side of that task: how an activity identifies the potential problems and hazards of running a data processing environment.

The risk analysis team begins by marking those assets critical to the activity's mission and adding those additional ones which might be very attractive to someone external to the activity. Someone may want the asset because of what could be gained by corrupting its internal contents, learning its function or meaning, or denying the activity possession.

With the assets just marked in mind, the team then considers all the potental threats that, if realized, could inflict damage. One starts by considering the possible adversaries that would take advantage of any opportunity to attack the activity. Basically, this means listing the most likely threat agents (natural environmental factors, authorized users, and hostile agents) and speculating on how they could hurt the activity.

To complete this review, it is prudent to ask where might each attack occur, such as at the computer mainframe, remote terminal, programming office, or tape library. Additionally, one should ask when might it happen: during normal working hours, on holidays, just after a shift change, or during an emergency such as a system crash, power failure, or fire. By doing this additional review, potential threat scenarios can be documented and evaluated.

Having listed every plausible threat scenario, the team determines how the potential attacks could harm the activity. This refers back to the four treat impact areas of modification, destructon, disclosure, and denial of

service. In addition to determining the impact area, an evaluation is made concerning how often a threat might be perpetrated. This evaluation accounts for the probability of each scenario occurring, given the existing ADP security posture of the activity.

In summary, one identifies threats by considering those threats that:

- have been known to occur at the activity in the past: machine failure, theft, system crashes, information loss and vandalism;
- might occur with some reasonable probability in the geographic area: fire, earthquake, and flood; and
- could result from accidental or intential errors of humans. [Ref. 22: p. 32]

As a starting point, some threats which are common to the current data processing environment have been listed in Table VI. Additionally, the impact area(s) associated with the realization of each threat is(are) marked accordingly. The examples are a representative sampling which the risk analysis team can use as a checklist of potential threat areas. For a more exhaustive threat evaluation the reader is encouraged to read Martin (1973), NBS FIPS 31 (1974), Ref. 20, and Ref 22.

TABLE VI

Common Threats and their Impact Areas

THREATS	Destruction	Disclosure	Modification	Denial of Service
Emanations/Eavesdropping	No	Yes	No	No
Alteration of Software	Yes	Yes	Yes	Yes
Alteration/Failure of Hardware	Yes	Yes	Yes	Yes
Unintentional Operator Error	Yes	Yes	Yes	Yes
Unintentional Data Entry Error	Yes	Yes	Yes	Yes
Unintentional System Programmer Error	Yes	Yes	Yes	Yes
Unintentional Disclosure	No	Yes	No	No
Misuse of Computer Resources	Yes	Yes	Yes	Yes
Power Instability	Yes	No	Yes	Yes
Telecommunications Failure	No	No	No	Yes
Environmental Control Failure	No	No	No	Yes
Natural Disaster	Yes	No	No	Yes
Water Damage (Internal/External)	Yes	No	No	Yes
Fire (Internal/External)	Yes	No	No	Yes
Enemy Overrun/Civil Disorder	Yes	Yes	No	Yes

[Ref. 10: p. E-46]

B. MANAGEMENT DECISION

In this phase of the Risk Management Program, activity top management judges whether the level of risk attributed to the data processing environment is acceptable.

Before making that judgement, top management appraises the risk analysis. This appraisal includes conducting a sensitivity analysis on the data used to substantiate the Total ALE and evaluating the technical merits of the overall analysis effort. The sensitivity analysis determines what effects changes in the estimated data can have on the Total ALE. The technical merits can be evaluated by asking the following types of questions.

- Did the users participate in estimating the loss expectancy of assets?
- Was the risk analysis team adequately skilled and experienced to make the appropriate assumptions?
- Are the results realistic and defensible?
- Can the results be replicated by another team?
- Were the calculations performed correctly?
- Were the existing countermeasures sufficiently considered in the analysis?
- Did the risk analysis team adequately consider the activity's mission and users' dependence on automated support?

If the results of the risk analysis are not acceptable, top management identifies the deficiencies in the analysis and reinitiates the Risk Analysis Phase. If the results are acceptable, top management approves the risk analysis.

After the risk analysis is approved, top management determines whether all mandatory countermeasures have been implemented. This is done by comparing the list of mandatory countermeasures with the existing ones documented during step 2 of the risk analysis.

Top management next evaluates the Total ALE. The decision of whether the Total ALE is acceptable depends exclusively on the amount of risk that top management is willing to assume, given the activity's mission and users' dependence on automated support. Many judge the level of risk as acceptable when the loss per year is so small that the activity's overall mission is not significantly degraded if threats are realized. Since each activity has a unique combination of assets, vulnerabilities, personnel, and security policies that establishes its data processing environment, no universally accepted ALE is appropriate for all activities. [Ref. 23: p. 2]

The pertinent decisions relative to this phase are modeled by the decision table in Table VII. The table is divided into two blocks (conditions and actions). The decision table is read by IF condition 1 AND condition 2 AND condition 3 are true, THEN take the action marked. When evaluating each condition listed, note that the column entries indicate the conditional states of satisfied (T), not satisfied (F), or has no bearing (-). The action block lists each decision relevant to the various conditional states. The action column entry "X" indicates the action to be taken while a blank implies no action required.

C. RISK CONTROL

1. Model

The Risk Control Phase is concerned with selecting additional countermeasures to improve the overall ADP security posture of the activity. Countermeasures are selected which reduce the frequency of particular threats, minimize the loss expectancy associated with particular assets, or provide an alternative means of automated support. Countermeasures are selected by an iterative

TABLE VII

Management Decision Model

Conditions	Risk Analysis Credible and Defensible	T	T	T	F
	Mandatory Countermeasures Implemented	T	T	F	-
	Total ALE Acceptable	T	F	-	-
Actions	Reinitiate Risk Analysis Phase				X
	Initiate Risk Control Phase		X	X	
	Initiate Operational Continuity Phase	X			

process, in which steps 2 and 3 of the Risk Analysis Model are repeated until the projected Total ALE is reduced to an acceptable level. This process is executed iteratively in order to ensure that the set of selected countermeasures is the optimal set.

There are several constraints affecting the process of countermeasure selection. The most significant constraint is the required selection of countermeasures which are designated mandatory by higher authority and must be implemented regardless of any other criteria. Higher authority is defined as the Designated Approving Authority and the organizational chain of command in the DON.

The second constraint is that each countermeasure should provide a positive return on investment. That is, the reduction in Total ALE (an annualized figure) as a result of the implementation of a countermeasure must be greater than the annualized cost of the countermeasure. The ammortized cost of the countermeasure is computed as the annual operating cost plus the annual portion of the one-time costs associated with that countermeasure. The annual portion of the one-time costs is the sum of the development, implementation, and/or installation costs, divided by the number of years in the anticipated life of the countermeasure.

The four step model of the risk control phase is presented in Table VIII, and described in more detail in Appendix E of Ref. 10. Step one is the examination of those countermeasures mandated by higher authority. Those countermeasures are placed at the top of the priority list for implementation. If the projected Total ALE with the mandatory countermeasures, is less than or equal to the maximum acceptable Total ALE, the Risk Control Phase is completed.

If the projected Total ALE after implementation of mandatory countermeasures is still not acceptable, additional countermeasures must be selected for implementation. The selection begins by finding the countermeasure which has the greatest potential of lowering the projected Total ALE. The process of selecting the next best countermeasure is repeated until the projected Total ALE is reduced to an acceptable level. The process is iterative because the amount of reduction associated with each countermeasure is dependent on the other countermeasures previously evaluated. This anomaly is similar to the "law of diminishing returns" when two countermeasures affect the same threat frequencies or loss expectancies.

TABLE VIII

Risk Control Model

Objective:

Choose C1 through Cj so that

TALE(E + M + C1 +...+ Cj) ≤ MATALE

By:

1. Survey all mandatory countermeasures.

   If TALE(E + M) ≤ MATALE, go to step 5.

2. Choose countermeasure C1 such that:

   TALE(E + M + C1) is minimized, and

   TALE(E + M) - TALE(E + M + C1) > Cost(C1).

   If TALE(E + M C1) ≤ MATALE, go to step 5.

3. Choose another countermeasure, Cj, such that:

   TALE(E + M + C1 +...+ Cj) is minimized, and

   TALE(E + M + C1 +...+ Ci) -
   TALE(E + M + C1 +...+ Cj) > Cost(Cj).

   If TALE(E + M + C1 +...+ Cj) ≤ MATALE,
   go to step 5.

4. Repeat step 3 until:

   TALE(E + M + C1 +...+ Cj) ≤ MATALE.

5. Develop Plan of Action for implementation of necessary* countermeasures.

- -

Where:

TALE(E + M) = Projected Total ALE with existing and mandatory countermeasures (annual)

MATALE = Maximum acceptable Total ALE

Cost(Cj) = Ammortized cost of countermeasure Cj

TALE(E + M + C1 +...+ Cj) = Projected Total ALE with existing countermeasures, mandatory countermeasures, and proposed countermeasures 1 through j

* Necessary means mandatory and additional

Finally, the optimal set of countermeasures is prioritized and scheduled for implementation. Top management is responsible for approving that recommended set of additional countermeasures and their implementation schedule. Those considerations addressing prioritization are provided in the following section.

2. Implementation Considerations

The objective of the Risk Control Phase is to provide an approved, prioritized optimal set of countermeasures which, when implemented, lower the Total ALE of an activity to an acceptable level. The task is not a simple one, and requires that management devote adequate resources in both expert manpower and time to accomplish it. Several considerations must be made during the selection of countermeasures for presentation to management.

The first consideration, as discussed above, is the selection of those countermeasures which are designated mandatory by high authority. The SPLICE network and individual SPLICE locations are required to implement those countermeasures listed in Appendix J of OPNAVINST 5239.1A [Ref. 10] and NAVSUPINST 5510.6A [Ref. 15]. Additional mandatory countermeasures may be identified in future revisions of the SPLICE Security and Risk Analysis Plan [Ref. 11].

The second consideration concerns the cost-effectiveness of each countermeasure. To be a candidate for selection, a countermeasure must have a postive return on investment. That is, the benefit realized by implementing the countermeasure must be greater than the ammortized cost of the countermeasure.

The final consideration in compiling a set of candidate countermeasures concerns the feasibility of each countermeasure. Those countermeasures which the risk

control team judges infeasible due to such things as geographic location or technical limitations should be documented as "considered, but judged infesible." Thorough documentation and management participation is crucial during this feasibility review to adequately address activity budgetary constraints. For those countermeasures judged feasible and practical, top management initiates the appropriate planning and budgeting support needed for their implementation.

To ensure that the optimal set of countermeasures is proposed, the risk control team analyzes the results of the risk analysis from several perspectives. The matrix of assets and threats is examined to identify those threats with the greatest potential for harm, in terms of their threat frequencies. Specific countermeasures should be considered which reduce the likelihood of those threats occurring.

Additionally, the team reviews the matrix to identify those assets with high loss expectancies. It is important to recall at this point that the loss associated with an asset is not limited to the replacement value of that asset, but is often compounded with the value of the service that the asset provides. Those countermeasures which minimize the loss expectancies associated with assets should be considered for implementation.

Finally, a global inspection of the risk analysis must be taken. During this inspection, top management relies on the technical expertise of the risk control team to "read between the lines" of the asset/threat matrix and to identify those vulnerabilities that allow a variety of threats to materialize. The forms required for the evaluation of countermeasures are provided in Ref. 10.

As explained in the Risk Control Model, proposed countermeasures are selected in an iterative process. Countermeasures are normally targeted to reduce the vulnerabilities of an activity and, when implemented, usually affect multiple vulnerabilities simultaneously. Due to this overlapping result, the effectiveness of a countermeasure must be evaluated with respect to the entire data processing environment before determining the total benefit that could be realized. Additionally, the implementation of a countermeasure could in some situations generate a more serious vulnerability than that which the countermeasure was intended to correct. In this situation, activity top management must decide if the benefit gained outweighs the weakness created. For example, a recommended software countermeasure might require multiple, lengthy passwords to improve access control. Unfortunately, passwords of this nature are often written down and taped to terminals, thereby negating the effectiveness of passwords and creating a greater vulnerability.

When the projected Total ALE with the additional countermeasures considered is less than the maximum Total ALE acceptable, the selection of countermeasures is completed. The next task of the risk control team is to develop a plan of action for implementing the set of selected countermeasures. The development of this plan will be guided by the availability and timing of those resources required for countermeasure implementation. When the set of proposed countermeasures and the implementation plan is approved by top management, the Risk Control Phase is completed.

Recent ADP security literature provides documentation on a variety of countermeasures. A discussion of many of those countermeasures is provided in the next chapter.

D. OPERATIONAL CONTINUITY

1. Model

Like the Management Decision Phase, the Operational Continuity Phase is modeled by a decision table. The table is applicable at any time during the phase, which can be as long as five years. Since the Risk Management Program requires continual review of the ADP security posture of the activity, the decision table should be consulted on a continual basis.

Some elements of the decision table, which is given in Table IX, deserve amplification. When an activity enters the Operational Continuity Phase, a request for accreditation is immediately forwarded to the DAA. If the activity has no countermeasures which must implemented, this initial request can also be considered a final request. If necessary countermeasures are to be implemented, then a final accreditation request will be submitted when their implementation is completed.

According to Ref. 10, an activity must conduct a risk analysis and be accredited every five years or whenever there is a significant change in the system configuration or facility. Therefore, a "Not satisfied" (F) in either of these conditions requires initiation of the Risk Analysis Phase, regardless of any other conditions. Finally, since the Operational Continuity Phase can be entered from either the Management Decision Phase or the Risk Control Phase, a likelihood exists that the implementation of countermeasures is happening simultaneously with the daily operation of the activity. The responsibilities and authorizations needed to implement the necessary countermeasures is addressed in the Implementation Considerations. When the Plan of Action for implementing the necessary countermeasures is completed, a request for final accreditation is submitted to the DAA.

TABLE IX

Operational Continuity Decision Model

Conditions	No significant change in configuration or facility	T	T	T	T	T	T	F	F
	< 5 years since last risk analysis	T	T	T	T	F	F	-	-
	Final accreditation has been requested	T	T	F	F	T	F	T	F
	All necessary countermeasures have been implemented	T	F[1]	T	F	-	-	-	-
Actions	Request Final Accreditation			X					
	Withdraw Accreditation request[2]		X			X		X	
	Continue Operational Continuity Phase	X	X	X	X				
	Reinitiate Risk Analysis Phase					X	X	X[3]	X[3]

[1] New mandatory countermeasures required by higher authority.

[2] Notify DAA about action initiated.

[3] The scope of the risk analysis would depend on the degree of change in configuration or facility.

2. Implementation Considerations

When this phase is entered, activity top management has approved the results of the Risk Analysis Phase, and, if the Risk Control Phase was executed, has approved a list of necessary countermeasures and their implementation plan. This review and approval documentation is submitted to the

DAA in support of an initial request for accreditation. Upon receipt of the request, the DAA will issue an activity accreditation that assigns each ADP system of the activity to one of the following three categories:

- ADP systems for which all cost-effective countermeasures have been implemented,
- ADP systems with an acceptable projected level of risk, but with some countermeasures not yet implemented (these systems will be granted an interim authority to operate pending implementation completion), and
- ADP systems with a unacceptable level of risk which requires that operations cease until corrective measures have been implemented. [Ref. 10: pp 3-2, 3-3]

As previously stated, the Operational Continuity Phase includes implementing the countermeasures approved during the Risk Control Phase (if any) and conducting an ongoing audit and security inspection of the activity ADP security posture. One individual must be assigned these responsibilities and given appropriate authority and resources to execute them. That person is designated the Activity ADP Security Officer and is the head of the ADP Security Staff. The responsibilities of both the ADP Security Officer and the staff are presented in detail in Chapter 2 of Ref. 10.

During the implementation of necessary countermeasures, the Plan of Action may require adjustments. To allow for this, there must be a responsive two-way communication between the ADP Security Officer and top management about real world considerations and constraints. Some reasons for modification might be unforeseen budgetary changes or required implementation of a new directed mandatory countermeasure. Additionally, the plan should be "tweaked" to minimize the disruption of daily operations.

When all necessary countermeasures have been implemented and a request for final accreditation has been submitted, the DAA evaluates the effectiveness of the new countermeasures by means of a Security Test and Evaluation (ST&E) [Ref. 10: p. 3-6]. After the ST&E, the DAA responds to the accreditation request by assigning each ADP systems to one of the three categories discussed above.

The Operational Continuity Phase is terminated when policy dictates that another risk analysis is required. At a minimum, the Risk Analysis Phase will be reinitiated when in the opinion of top management there has been a significant change to the configuration (hardware or software) or facility, or when there has been a lapse of five years since the last approved risk analysis.

IV. TECHNICAL AND MANAGERIAL COUNTERMEASURES

As stated previously, the current data processing environment is viewed as a collection of assets. To protect these assets, various technical and managerial security mechanisms are implemented. Technical countermeasures are those internal hardware, software, and communication protection mechanisms that are peculiar to the ADP system and are best addressed in the overall system design specifications. Managerial, also called conventional, countermeasures are those administrative, personnel, and physical mechanisms that are commonly required for the protection of any environment, automated or not. Managerial countermeasures are implemented throughout the system's life cycle and are often used to enhance the effectiveness of technical countermeasures.

The ADP security policies which industry enforces through the implementation of technical and managerial countermeasures are:

- all users and devices require positive unique identification and verification (authentication).
- all interactions involving users, devices, and other named system elements will be controlled by an authorization strategy (access control).
- all activity within the ADP system should be observed so that users (authorized or not) can be detected and held accountable for their actions (surveillance).
- all elements of the ADP system will function in a cohesive, identifiable, predictable, and reliable manner so that malfunctions are detected and reported within a known time (integrity).

The countermeasures discussed in this chapter are organized by the four ADP security policies presented above. The countermeasures are not identified specifically as technical or managerial because a combination of both is required to enforce an adequate ADP security policy. For example, the authentication policy is often achieved by implementing passwords. For passwords to be effective, they require a software mechanism to accept and recognize passwords and an administrative control to properly distribute and audit their usage.

A. AUTHENTICATION

Authentication countermeasures prohibit the use of system resources by unauthorized users or devices by verifying the unique identity of the user or device before servicing a request.

1. User Authentication

User authentication is essentially a two-step procedure of identity definition and identity verification. In the first step, the user provides his or her user identification number and password during initial log-on to the system. In the second step, the system performs a table lookup and verifies that the password provided correctly maps to the user identification number. Additionally, administrative controls ensure that each identification number/password combination is assigned to only one user, and that the user has not provided his or her unique number and password combination to someone else.

User authentication can be performed to some extent at the physical security level by such controls as: guards stationed at physical entry points, personnel sign-in/sign-out logbooks, and closed-circuit monitors.

These physical security countermeasures are not sufficient at the ADP system level, particularly if the system supports remote terminals or network communications. As an example, when a user submits a batch job to the data processing center in person, his or her identity can be verified. When that same batch job is submitted from a remote terminal, the user's identity is no longer assured.

There are three methods for verifying a user's identity. These methods, which can be applied singly or in combination, are based on:

- something the person knows (e.g., a password, a combination to a lock, or a fact about the user's personal background);
- something the person has (e.g., a badge, a key to a lock, or a card with machine readable information); or
- something the person is (e.g., his or her signature, speech, hand geometry, or fingerprints). [Ref. 24: pp. 8-10]

Several commercially developed devices for recognizing personal attributes such as fingerprints or hand geometry are available. However, the cost of implementing such countermeasures make them impractical for most decentralized data processing environments like the SPLICE Network. The practicality of their implementation depends on the cost of the countermeasure in relation to the amount of protection needed to lessen the activity's potential losses.

The most widely accepted countermeasure for enforcing an authentication policy is the assignment of a unique user identification number and password. The user number is entered via a badge or card, or entered from a keyboard, whereas the password is generally entered only from a keyboard. In addition to its use in authentication,

the user's identification number is also used in maintaining a journal of his or her activities. Passwords, unfortunately, have many potentially damaging vulnerabilities. Some technical and managerial countermeasures that have been recommended by Courtney [Ref. 3: pp. 40 -43,], NBS [Ref. 24: pp. 9 - 12], and Shanker [Ref. 25: p. 30,] as appropriate to counteract the vulnerabilities of passwords are as follows.

- Password Generation and Selection - Passwords should be comprised of a sufficient number of characters and generated in such a manner as to assure a degree of protection commmensurate with the value of the assets. They should be generated randomly, so that no association with a particular user can be detected. Berman has suggested that password generation be based on the concept of a "virtual password" [Ref. 26: pp. 97-104]. The password is created at the time the user identifies himself or herself to the system and is based on the user's identification number, social security number, and, in some cases, the user's department number. Ref. 26 also provides a sample algorithm that is suitable for generating a "virtual password."
- Password Distribution - Passwords for accessing the ADP system should be distributed only to users meeting the ADP system's need-to-know and need-to-utilize criteria. The use of a unique password by a user to access the the ADP system, the application system, and the network is endorsed by industry and is used by several command and control ADP systems within the Navy. This hierarchy of access requires that the user be authenticated at the system, application, and network levels. Each password should be personally delivered to a user with instructions to memorize it, or it should be transmitted over a secured communication path to the user. If the password

is transmitted, then either the user should immediately initiate a password change or, if implemented, an automatic password change routine should be invoked after initial log-on.

- Password Storage Protection - Passwords are usually stored in a file located in main memory. The file is therefore vulnerable to tampering. To protect the password file, an appropriate countermeasure is to either encrypt the file using the Data Encryption Standard (see Ref. 27) or pass the file through a hard-to-invert transformation algorithm. The algorithm should be sufficiently difficult to prevent a code breaker from successfully breaking the code with a reasonable amount of time and resources.
- Password Usage Protection - Passwords entered via CRT or printing terminals should be prevented from display by masking the keyboard response. Additionally, a security alarm or a terminal lockout should be generated automatically after a specific number of unsuccessful access attempts or a specific time delay has elapsed since the last access attempt. In order to uncover possible unauthorized usage of a password, it is suggested that each user be shown a record of the most recent accesses under his or her password upon log-on. To protect passwords during a communications transmission, an appropriate countermeasure is to use either an encryption technique or a protected communications distribution system [Ref. 10: p. F-39]. The system should also respond in the same manner to a valid identification number and invalid password, as it does to an invalid identification number and invalid password. This prevents a user, who is attempting an unauthorized access, to know whether the identification number is valid or not.

- Password Lifetime - Passwords should be changed periodically, since the likelihood of them being surreptitiously discovered increases with time. Also, if a password is compromised or a user's access right is revoked, then the password should be immediately invalidated.

2. Device Authentication

Besides authenticating an authorized user, the ADP system should be able to uniquely recognize devices that are requesting services. This is particularly important when evaluating the threats posed by remote or portable terminals. An appropriate technical countermeasure is to require each device to be equipped with circuitry which will respond automatically to an interrogation command and transmit an identification code. This handshaking between the ADP system and the remote device is accomplished either by an exchange of identification codes or by the successful execution of a particular algorithm. The identification code, also called a security code, should identify the particular device and be unique within the system. This permits a system-wide journal to maintain a log of accesses by device. The device's circuitry should be protected in tamper-resistant housing, and, if the amount of protection warrants, the transmission should be protected by encryption or a protected communications distribution system. [Ref. 24: p.22]

If the system services devices which are not directly connected, it should be capable of initiating a call-back procedure that verifies the device's identity. This call-back procedure makes use of a remote access list, which must include device identification codes and a set of authorized logical addresses or telephone numbers from which each device can originate a request. Implementing either of

these countermeasures will enable the ADP system to guard against an unauthorized device masquerading as an authorized one.

B. ACCESS CONTROL

Access control countermeasures enable properly identified users to access only those system resources for which authorization has been granted. Traditionally, authorization in conventional systems has meant that every system element is automatically granted access to every other system element, unless specifically prohibited. In contrast, ADP systems base authorization on the "least privilege" principle, which states that a system element is expressly prohibited from accessing another element, unless authorization has been explicitly granted. This principle limits the damage that can result from error or malicious attack and restricts the access of system elements to a protective domain.

Before discussing the design considerations for access control mechanisms, an explanation is required of what constitutes a subject and an object. A subject is an active entity in the ADP system that corresponds to a process or task acting on behalf of a user or the operating system. An object is either a software created entity which represents a collection of information (e.g., file, directory, or program) or a hardware recognizable entity like a terminal or special-purpose register. An access matrix conceptually represents what subjects can access what objects and specifies what access rights (read, write, delete, etc.) the subjects have to the objects.

1. Access Control Design Considerations

The design of access control mechanisms is based on three considerations: [Ref. 28: pp. 192-217]

- Access Hierarchies, which automatically give privileged subjects a superset of the access rights of nonprivileged subjects. Privileged subjects are those active entities of a two-state machine that operate in the supervisor domain. A subject operating in this domain has access to all objects in the system, can create and delete objects, initiate and terminate user processes, and execute privileged instructions not available to subjects operating in the user domain (nonprivileged subjects). For example, processes in the supervisor domain can change process status words and execute I/O instructions, while those in the user domain can only request those services be provided on their behalf.
- Authorization Lists, which associate with each object those subjects which have access rights to it. These lists are typically used to protect owned objects such as files and data.
- Capabilities, which are like "tickets" for objects; possession of a capability unconditionally authorizes the holder access for all associated objects. In other words, associated with each subject is a capabilities list which specifies the subject's access rights to a list of objects.

Access control can be segregated into several levels: system, subsystem, file, record, or field, where the subject's access rights are delineated at each level. With an access control mechanism designed to mediate accesses down to the field level, a greater likelihood exists of detecting a violation or misuse of system resources.

However, such a design significantly increases the number and types of accesses to be verified and generally leads to a degradation of system performance.

2. Access Control Implementation

Access control countermeasures are implemented by software routines which execute in the supervisor domain, and are invoked by the file manager to grant or deny access when symbolic references are made between subjects and objects. As shown in Figure 4.1, the access control matrix identifies all subjects and objects in the system and defines their relationship. If the matrix were directly implemented, the time required to validate an access request could be unreasonable due to the potentially large number of empty spaces in the matrix.

Depending on the system software design, the access control countermeasure, which enforces the relationships depicted in the matrix, can be implemented in different ways. One approach is to organize and store the access relationship from the subject's perspective, thereby eliminating empty spaces in the matrix. This perspective, which is called a capability-list orientation, maintains a capability list for each subject giving both the subject's access rights and its related objects. The advantage of this approach is that once the subject's capability list is retrieved, the time required to validate subsequent access requests is minimal. [Ref. 28: pp. 207-218, Ref. 29: p. 169]

A second approach is to organize and store the relationship from the object's perspective, where once again the empty spaces are eliminated. This perspective, which is called an authorization-list orientation, maintains with each object a list of authorized subjects and their respective access rights. The advantage of this approach is that

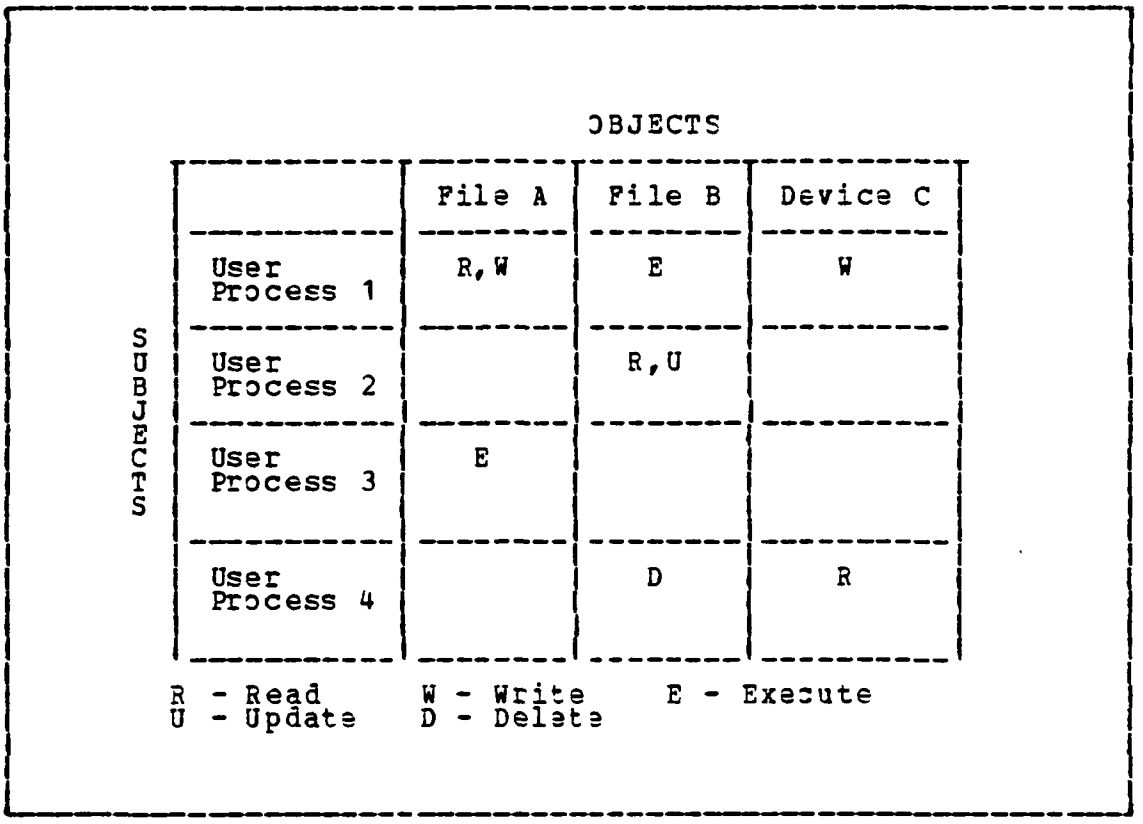


Figure 4.1 Access Control Matrix.

once an object has been requested, further requests for the same object can be readily processed. [Ref. 29: p. 169]

Each of the approaches discussed above has a serious maintenance problem. For example, when an object is removed or a subject's access rights are changed, an exhaustive search is needed to update all affected entries. This is very time consuming when using a list based strictly on either capabilities or authorizations. Ref. 29 recommends an authority-item approach to overcome this deficiency. The approach is explained as a method for

> organizing the access control information into authority items, each of which corresponds to a user (subject). Furthermore, every resource (object) in an authority item is linked with the same resources (objects) in

other authority items. Thus, the authority item approach supports capability lists directly and access (authorization) lists indirectly through linkages. In this way, search of authority items due to removal, changes, and suspensions need not be exhaustive. [Ref. 29: p. 170]

Regardless of the approached pursued, the overriding consideration is to reduce the time needed to grant or deny an access request and to provide a flexible mechanism that can readily adapt to the dynamic interaction between subjects and objects. For additional information on different implementations of access control countermeasures, the works by Stiegler (1979), Buttar (1980) and Gladney (1975) are recommended.

The implementation approaches presented above were directed towards alternative design proposals for the access control function. These same considerations apply equally as well to the design of a data base management system since it also is concerned with ensuring that only authorized users gain access to resources [Ref. 30: pp. 229-252].

C. SURVEILLANCE

The surveillance countermeasure detects and reacts appropriately to any internal system activity that it has determined may constitute a security threat. In order to determine the source of this threat, the system must have a means of achieving strict personal accountability for all users (unique assignment of identification numbers). A surveillance countermeasure needs the capability to concurrently perform two functions: threat monitoring and security auditing. For the countermeasure to be effective, the events to be monitored and logged must be approved during the design of the ADP system and the capability implemented prior to its operational use. The surveillance countermeasure is usually implemented to operate in the

privileged domain and, like all other system software, requires protection from unauthorized modification, destruction, disclosure, or denial of service.

Threat monitoring is the real-time detection of a successful or attempted penetration of the ADP system. The threat monitor observes all user and system interactions to ensure that the proper actions and responses are being exchanged. If the monitor detects a security violation (penetration attack), it must record the event and take some automatic action, depending upon the severity and effect of the violation. This action could range from printing a security alert message on the operator's console to sounding an alarm in the ADP Security Officer's location. In designing the monitor, one must address what information, if any, should be returned to the user attempting to compromise the system and what the disposition of the user's program should be if execution had been initiated.

Security auditing concerns the logging, analyzing, and reporting of security-related events, in particular, any attempted or successful security violation. The logging function collects and records in a historical file such things as the user's identification number and time of log-on, the devices from which the user has entered commands, programs, and files, and any other system data unique to the particular user session (e.g., general registers, memory bounds, location of virtual memory table) [Ref. 29: p. 166]. The logs are used to provide an audit trail of system activity and to assist in the investigation of recorded security violations.

Analyzing and reporting of security-related events is a joint responsibility of the surveillance software countermeasure and the ADP Security Officer. The countermeasure is normally designed to maintain statistics on security-related events and to prepare standardize reports on such events,

while it is the ADP Security Officer that interprets these products and takes appropriate actions to correct the documented vulnerabilities. It is intended that a surveillance countermeasure will act as an effective psychological deterrent to the user who might otherwise consider abusing his or her privileges.

D. INTEGRITY

Integrity is the quality of protection that assures that the ADP system works in a cohesive and predictable manner regardless of the operating conditions, that technical countermeasures are effective in maintaining the desired security level, and that the ADP system is adequately protected from the occurrence and impact of errors [Ref. 31: pp. 15-17]. Countermeasures for enforcing a system integrity policy include controls for the internal (hardware and software) system, processing, and system errors. The technical countermeasures presented in the following sections have been synopsized from Refs. 29, 32 and 33. The listing is by no means exhaustive, rather it repesents industry's judgement of the most effective countermeasures for today's hardware and software. These countermeasures are not usually identified explicitly as security mechanisms, but are often present for assuring a high degree of system reliability.

1. Internal System Controls

In today's multiprogramming and multiprocessing ADP systems, many users are concurrently sharing system resources (memory, CPU, and I/O devices) and programs. The multiplexing of these elements among many users has created a need to isolate (self-protect) user programs from one another, the system software, and the other system

resources. This isolation of elements is achieved by implementing various technical countermeasures that provide for main memory protection, dual execution states, and virtual machine monitors.

a. Main Memory Protection

Main memory protection concerns the ability to protect partitions or portions of main memory from unwarranted access by user programs. Main memory is usually divided into mutually exclusive areas that are managed by the system software. The system software loads these areas with as many user programs as can be efficiently serviced. In previous generations, this meant bringing in a user program, executing it for a period of time, suspending its execution, and loading in another user program. This swapping continued usually via a round robin servicing scheme until the user program had finished execution. This is no longer judged as an efficient use of main memory.

To overcome this inefficiency, a new architecture developed which supports a virtual memory capability. The important characteristic of a virtual memory architecture is that the address space of a user program is partitioned into a set of independently allocated units, some of which are main memory resident during program execution, and some of which are not. With this new approach, the system software loads only units needed for execution, hence a greater number of users can be serviced and memory usage is more efficient. [Ref. 32: pp. 32-33]

When the ADP system does not permit concurrent sharing of system resources or processes by multiple users, the traditional main memory protection countermeasures of base and bound registers or locks and keys are sufficient to enforce an isolation policy. Memory base and bound registers are set by the system software to specify the valid

upper and lower main memory addresses for the currently executing process. Any attempt by the process to fetch from or store to an address outside these bounds generates an interrrupt to the system software. When a different process is brought in, the base and bound registers are changed to describe the new process' memory area. A lock and key countermeasure is implemented by marking each location in main memory with a lock and each program with a key. When the user program is brought into main memory for execution, the system software compares the key with the locks and unlocks only those areas matched by the program's key. Each fetch and store is automatically examined by the hardware to confirm that the key and lock match.

When the ADP system permits resource sharing, these traditional countermeasures are not adequate because they allow programs with different protection attributes to concurrently access the same area of main memory. Ref. 29 recommends a solution to this problem that incorporates the protection attributes and size contraints in the address translation table. This table is used by the system software to map the virtual addresses of a user program into the physical addresses needed in main memory. [Ref. 29: pp. 108-114]

Some additional countermeasures that are needed to protect ADP systems which process sensitive business data are as follows.

- Ability to scrub (zero out) residue from main and secondary memory before reallocation to another user process.
- A memory write protection feature that prevents one program from overwriting another. Any attempt to write generates a system interrupt.

b. Dual Execution States

The dual execution states of privileged and nonprivileged allow the CPU to maintain the two execution domains of supervisor and user. The system software executes in the supervisor domain, thus it is permitted immediate access to all system resources, including the ability to execute privileged CPU and I/O instructions. On the other hand, the user's process executes in the user domain and any attempts to execute a privileged instruction is automatically trapped by the CPU. Basically, this action generates an interrupt which signals the CPU to change to the privileged state and allows the system software to execute the instruction on behalf of the user process. This countermeasure is available on almost all current ADP systems.

c. Virtual Machine Monitors

The implementation of virtual machine monitors allows each user program to have its own virtual machine uniquely configured for its needs. The virtual monitor is considered to be a functionally complete machine with its own virtual CPU, memory, I/O channels, devices, and any other virtual resources requested. The only thing it lacks to execute a user program is the physical CPU. The physical CPU is allocated between virtual monitors, working a specific amount of time for each virtual CPU according to a specified strategy. This allows for the time-multiplexing of each virtual monitor on the actual hardware and the dynamic reconfiguration of the system to satisfy the needs of a user program. Since each user process is contained in a specifically configured virtual environment, any attempt to access a system resource outside that environment automatically generates a system interrupt. Therefore virtual

machine monitors also contribute to an isolation (self protection) security policy.

2. Processing Controls

Processing controls are mainly limited to administrative countermeasures such as standard operating procedures and software engineering practices that indirectly protect the ADP system and enhance the effectiveness of the technical countermeasures. Some of the controls that should be considered as possible candidates are as follows.

- Users should be restricted to programming only in higher-level languages.
- Modifications to system and application software should be implemented by a two-person control strategy. Two persons must sign off on all changes to the system software before the changes are made in the operational version.
- A Configuration Management Plan which addresses software development and maintenance procedures should be implemented.
- A Contingency Plan which describes the security procedures for responding to abnormal operating conditions should be established, published, and periodically tested.

3. System Error Controls

System errors, also called failures, result in a degraded or unknown performance level and can be caused by hardware malfunctions, software errors, or operator errors. Hardware malfunctions are caused by such things as the CPU, memory parity, I/O interface and communication line, or power failure. Software errors are concerned with both operating and application systems deficiencies and are

attributed to incomplete design specifications and/or implementation. And lastly, operator errors result from either badly defined operating procedures or simple human error. [Ref. 33: pp. 104-105]

In developing countermeasures to protect against these three types of errors, the designer must consider error prevention, detection and recovery. Error prevention is usually satisfied by providing sufficient redundancy so that a component failure does not degrade performance. Error detection requires the ADP system to be capable of recognizing potential hardware and software malfunctions before the entire system halts. Error recovery relates to continuation of system functions after an error has occured. Recovery can be affected at several levels, depending upon the severity and impact of the error. For example, if an error could crash the system, the recovery would be a system restart; or if a program attempted to read past the end-of-file, the recovery would entail an error message to the user. Some countermeasures that have been suggested by Carroll [Ref. 20: pp. 265-287] and TRW Systems, Inc. [Ref. 33: pp. 129-173] as effective in counteracting system errors are:

- hierarchically designed fault-tolerant ADP systems
- redundancy of hardware and software components
- automatic backup hardware switchover
- transfer of critical system functions from software to firmware or hardware
- dynamic checking of the system's operating state with appropriate recovery actions specified should an illegal state be detected
- capability for logical consistency checks (e.g., simultaneous interrupt prevention, device address and existence check, and time check on propagation of signals between

devices) with appropriate recovery actions initiated should an inconsistency be realized

- capability for selective termination, graceful degradation, automatic initiation of diagnostics, and graded (warm/cold) restarts
- memory parity and address validation
- replication of critical system files including data bases and audit logs
- employment of data integrity controls such as: checks for reasonableness, consistency, and range, use of checksum totals and parity during data transfers, and maintenance of a transaction journal
- timing and sequence checks pertinent to I/O operations (e.g., I/O instruction execution and I/O transmission)

V. RECOMMENDATIONS

A. RECOMMENDED SPLICE FUNCTIONAL SECURITY MODULE

This section provides recommended design specifications for a software Security Module to be incorporated into the functional design of the SPLICE Local Area Network (LAN). The specifications are based upon the assumption that all data handled within the SPLICE LANs will be classified no higher than Sensitive Business Data. The design specifications recommended in this section satisfy the protection requirements set forth in Refs. 10 and 11.

As discussed earlier, a complex data processing environment like SPLICE is usually protected by enforcing the four ADP security policies of authentication, access control, surveillance, and integrity. The SPLICE Security Module has been designed as a collection of submodules, with a recommended software submodule for each policy area except integrity. The integrity requirements of SPLICE have already been addressed in Ref. 13 and, if implemented, will be adequate. The integrity requirements address such things as memory protection features, change control procedures, memory parity, data integrity controls, and system consistency checks. The recommended security module is specifically tailored to satisfy the security requirements of the SPLICE LAN and should not be construed as being endorsed for all such environments. The terms used to describe the Security Module and its interactions with the other functional modules of the SPLICE LAN have been taken from Ref. 34.

The functions of the SPLICE Security Module are as follows:

- Authentication of the user when accessing the SPLICE Configuration.
- Authentication of terminals and peripheral devices when requesting or performing a service.
- Maintenance of an access control mechanism which enforces the access rights as prescribed for subjects and objects of the local SPLICE Configuration and validates requests for access to the SPLICE LAN and the Defence Data Network.
- Maintenance of an online security auditing mechanism that logs appropriate security related information required to support subsequent analysis efforts.

1. Authentication

In order to enforce an authentication policy, authorized use of SPLICE resources must be controlled by both an administrative and a software countermeasure. The administrative countermeasure requires that each user and device be uniquely identifiable within the SPLICE LAN. The software countermeasure necessitates the design of software submodules which function to identify users, terminals, and peripherals.

Chapter IV presented in detail numerous mechanisms considered effective in protecting a password authentication countermeasure. It is recommended that those mechanisms be evaluated for their applicability to the detailed design of the authentication submodule.

a. Authentication of Terminals and Users

The software submodule for authenticating terminals and users should be invoked by the Front End Processor (FEP) Module when the user initially attempts to log on to the local SPLICE configuration (local system). It is assumed that the FEP Module can recognize when a user is logging on to the local system and that it can invoke the submodule when appropriate.

The terminal's identity should be checked by requiring the terminal to transmit a security code in response to an interrogation command. The code is then matched against a table of authorized terminal security codes. If a match is found, the logon procedure continues. Otherwise, the security auditing submodule (to be addressed later) is invoked and appropriate actions for responding to a security violation are taken. After the terminal's identity is verified, the user's identification number and password are checked in a similar manner. If a match is found, the logon procedure is completed and control passed back to the FEP Module. If no match is found, the security auditing submodule is invoked as before and control is passed back to the FEP Module after appropriate actions have been taken.

It is recommended that the authentication submodule for terminals and users be located in the same physical machine as the FEP Module for each local system. This recommendation is based on the need to restrict a nonverified terminal and user to as little of the local system as feasible. This submodule will only be invoked when a user (local, remote or satellite) initially logs on to the local system.

b. Authentication of Peripherals

The authentication submodule for verifying the identity of a peripheral device has not been examined due to the lack of detailed design specifications concerning how the Peripheral Management (PM) Module interacts with the local system. Once the design has been completed, it is recommended that the countermeasures presented in Chapter IV Section A.2 be reviewed for their applicability.

2. Access Control

After the user's identity is verified, the FEP Module forwards all subsequent user messages to the Terminal Management (TM) Module. The TM Module responds by requesting that the Session Services (SS) Module establish and maintain a user session. After a session has been established, the SS Module examines each user request and invokes the appropriate generalized functional module needed for accomplishing the task requested. It is recommended that the SS Module invoke the access control submodule to validate the user's authorization rights before it invokes any other functional module on behalf of the user.

The access control submodule should perform two types of authorization control. First, if the user task requests access to the SPLICE LAN or the Defense Data Network, the access control submodule should ensure that the user has been authorized such an access. The second type of control involves granting or denying a user (either local, remote or satellite) access to a local system object such as a file, directory, or peripheral device to perform some action such as read, write or execute on that particular object. If the request is not allowed, the security auditing submodule is invoked and appropriate action is taken.

The design of the access control submodule should be based on the authority item technique presented in Ref. 29. This design specification reduces the time required to grant a user authorization request and allows authority items to be easily modified when changes are made to the authorization rights of a user (subject) or the access capabilities of an object. The implementation of this countermeasure requires that the authorization rights of users and access capabilities of objects be explicitly defined and maintained online for use by the access control submodule. It is recommended that the access control submodule be colocated with the SS Module to minimize the time required to validate a user's authorization.

3. Surveillance

In order to enforce a surveillance policy, it is recommended that a security auditing submodule be incorporated in the design of the SPLICE Security Module. No particular location for this submodule is recommended, as it could be a candidate for relocating from one physical machine to another as necessary to improve the overall performance of the SPLICE Configuration. This submodule will be invoked by the TM Module, the SS Module, the PM Module, and any other module which can recognize a security violation or system error. The appropriate actions for the submodule to take when invoked are to log the event, to notify the central system operator that an error or violation has occurred, and if the error or violation is severe enough, the user's log-on or session should be terminated. The security-related information recorded by this submodule should include at a minimum the following.

- A system access log which identifies who accessed the system, what terminal the access was made from, whether

the access attempt was successful, and the date and time it occurred.

- An input/output log which identifies who requested the service, what function (read, write, enter, print) was provided, whether the function was successful, and the date and time it occurred.
- A processing log which records appropriate security-related information about system errors and security violations.

B. OTHER RECOMMENDED SPLICE SECURITY MEASURES

It is recommended that NAVSUPINST 5510.6A be revised and reissued to accomodate the minimum mandatory countermeasures listed in Appendix J of Ref. 10, which was issued subsequent to NAVSUPINST 5510.6A. This would allow the mandatory countermeasures to be included by reference in the next version of the SPLICE Security and Risk Analysis Plan [Ref. 11].

The "SPLICE unbrella" contains many software products which are being developed by Central Design Activities for distribution to multiple activities. It is recommended that the SPLICE Project Officer insure that each software product is certified in accordance with OPNAVINST 5239.1A prior to distribution [Ref. 10: p. 3-1].

In the design of software products, the software controls listed in Appendix I of Ref. 10 must be incorporated. It should also be noted that contractor developed software and countermeasures are also subject to the requirements of Ref. 10.

It is recommeded that the following actions be taken to help insure that the risk in SPLICE is quantified and managed at an acceptable level.

- A Network ADP Security Officer should be designated early in the lifecycle of the SPLICE Project. The individual

so designated should be given a position high enough in the project organization and appropriate authority and resources to manage the SPLICE Risk Analysis Program and effect the necessary design changes and operational requirements.

- The Network ADP Security Officer should develop and maintain a comprehensive checklist of threats which are potentially present at any SPLICE activity. The reader is invited to review the works of Martin (1973), NBS FIPS 31 (1974), Ref. 20, and Ref. 22 for recommended lists of threats. The checklist should be made available to activity risk analysis teams.
- The Network ADP Security Officer should be given cognizance of all activity security incident reports [Ref. 10: p. 8-2] in order to identify and monitor vulnerabilities which potentially exist in the SPLICE Network.
- A risk management training program should be established to provide a consistent Risk Management Program throughout the SPLICE Network. A list of responsibilities for ADP security training is provided in Chapter 10 of Ref. 10.
- The appropriate Inspector General review program for every SPLICE activity should incorporate a security review, as defined in OPNAVINST 5239.1A [Ref. 10: p. 8-1].

C. FUTURE RESEARCH QUESTIONS

1. Validation of Security Module Specifications

This thesis provides a formal program for risk management, but does not attempt to quantify the risk in any particular activity. Additional research should be accomplished in at least one of several ways. The risk of operating can be estimated by simulating a "typical SPLICE

activity." This would require complete enumeration of all assets in the seven resource categories, and a listing of all "potential" threats facing a SPLICE activity.

Another research method would be to examine an existing Navy activity that is designated to become a SPLICE activity. By evaluating the changes in the data processing environment due to the SPLICE configuration, their impact on the ADP security posture of the activity can be properly examined.

By using one of these research methods, the recommended Security Functional Module can be validated and, if needed, additional countermeasures can be specified for in the design of the SPLICE software or implemented at the operational SPLICE activities.

2. Critique of Risk Management Program

The Risk Management Program models presented in Chapter 3 formalize the concepts proposed by Courtney [Ref. 3], NBS [Ref. 17], and Fitzgerald [Ref. 19], and adopted by the Navy in the DON ADP Security Program [Ref. 10]. Although the models presented here reflect the established concepts of the various references, no attempt has been made to analyze the validity of the concepts.

Both the Asset Loss Determination Model and the Threat and Vulnerability Evaluation Model are essentially exponential utility functions, which exhibit decreasing marginal utility. With respect to asset losses, this implies that an asset loss of $1,000 with a total asset loss level of $10,000 is not as significant as an asset loss of $1,000 when the asset loss level is at $100,000. A simple question arises in this reasoning. To a computer system user, is the tenth day of doing without service less important than the first or second? Likewise, is losing the use of a tape drive less significant if you have already lost

five tape drives than it is when you have lost none? There may exist an argument that the marginal utility should increase with increasing asset losses.

In threat and vulnerability evaluation, less significance is similarly placed on marginal risk as the activity becomes more vulnerable or more threats are present. Is the risk of a fourth or fifth attack not as significant as the second or third?

Finally, the Navy's risk management decision problem should be more fully modeled. Currently explicit constraints are placed on the activity manager by the DAA who sets a maximum acceptable Total ALE. Although not documented in the Navy program, the setting of the maximum acceptable Total ALE is done by use of the DAA's utility function. Certainly this choice is made in light of other investment alternatives, and with regard to the Navy system of incentives, rewards, and penalties.

APPENDIX A
LIST OF ACRONYMS

ADP	Automatic Data Processing (See EDP)
ADPSO	Automatic Data Processing Security Officer
ADPSSO	Automatic Data Processing System Security Officer
ALE	Annual Loss Expectancy
ARPANET	Advanced Research Projects Agency Network
CPU	Central Processing Unit
CRC	Cyclical Redundancy Check
CRT	Cathode Ray Tube
DAA	Designated Approving Authority
DDN	Defense Data Network
DES	Data Encryption Standard
FIPS	Federal Information Processing Standard (National Bureau of Standards)
GAO	General Accounting Office
I/O	Input/Output
IP	Internet Protocol
IPLI	Internet Private Line Interface
LCN	Local Computer Network

MC	Monitoring Center
NBS	National Bureau of Standards
NSO	Network Security Officer
OMB	Office of Management and Budget
SPLICE	Stock Point Logistics Integrated Communications Environment
ST&E	Security Test and Evaluation
TASO	Terminal Area Security Officer
TCP	Transmission Control Protocol
VMM	Virtual Machine Monitor

APPENDIX B
DEFINITIONS

The majority of the definitions contained herein are taken from the Department of the Navy Automatic Data Processing Security Program Manual, OPNAVINST 5239.1A [Ref. 10]. All definitions not from OPNAVINST 5239.1A are referenced.

ACCEPTABLE LEVEL OF RISK. A judicious and carefully considered assessment by the appropriate Designated Approving Authority (DAA) that an automatic data processing (ADP) activity or network meets the minimum requirements of applicable security directives and the provisions of OPNAVINST 5239.1A. The assessment should take into account the value of ADP assets; threats and vulnerabilities; countermeasures and their efficacy in compensating for vulnerabilities; and operational requirements.

ACCESS. The ability and the means to approach, communicate with (input to or receive output from), or otherwise make use of any material or component in an ADP system. Personnel only receiving computer output products from the ADP system and not inputting to or otherwise interacting with the system (i.e., no "hands on" or other direct input or inquiry capability) are not considered to have ADP system access and are accordingly not subject to the personnel security requirements of OPNAVINST 5239.1A. Such output products, however, shall either be reviewed prior to dissemination or otherwise determined to be properly identified as to content and classification. [Ref. 35]

ACCESS AUTHORIZATION. Password and/or user id required to meet security restrictions for the resource being accessed. [Ref. 13]

ACCREDITATION. A policy decision by the responsible DAA resulting in a formal declaration that appropriate security countermeasures have been properly implemented for the ADP activity or network, so that the activity or network is operating at an acceptable level of risk. The accreditation should state the mode of operation and any operating limitations applicable to the ADP activity or network.

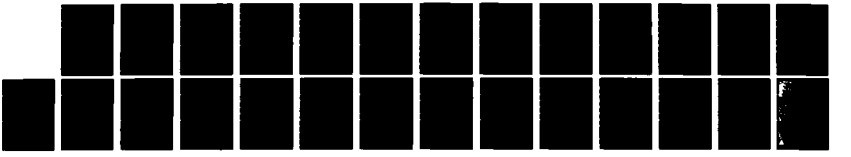
ADMINISTRATIVE SECURITY. The management constraints; operational, administrative, and accountability procedures; and supplemental controls established to provide an acceptable level of protection for data. Synonymous with procedural security. [Ref. 36]

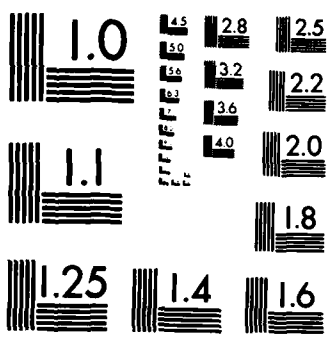
ADP ACTIVITY. Any organizational entity with responsibilities for developing, operating, or maintaining an ADP system or network.

ADP SECURITY. Measures required to protect against unauthorized (accidental or intentional) disclosure, modification, or destruction of ADP systems and data, and denial of service to process data. ADP security includes consideration of all hardware/software functions, characteristics, and/or features; operational procedures, accountability procedures, and access controls at the central computer facility, remote computer, and terminal facilities; management constraints; physical structures and devices; and personnel and communication controls needed to provide an acceptable level of risk for the ADP system and for the data or information contained in the system.

AD-A127 631 PROPOSAL FOR STOCK POINT LOGISTICS INTEGRATED COMMUNICATIONS ENVIRONMENT (.. (U) NAVAL POSTGRADUATE SCHOOL MONTEREY CA S K CROWDER ET AL. DEC 82 2/2

UNCLASSIFIED F/G 15/3 NL





MICROCOPY RESOLUTION TEST CHART
NATIONAL BUREAU OF STANDARDS-1963-A

ADP SECURITY STAFF. Individuals assigned and functioning as action officials for ADP security within their respective organization:

ADP Security Officer (ADPSO)
ADP Systems Security Officer (ADPSSO)
Network Security Officer (NSO)
Terminal Area Security Officer (TASO)
Office Information System Security Officer (OISSO)

ADP SYSTEM. An assembly of computer equipment, facilities, personnel, software, and procedures configured for the purpose of classifying, sorting, calculating, computing, summarizing, storing and retrieving data and information with a minimum of human intervention. An ADP system as defined for purposes of OPNAVINST 5239.1A is the totality of automatic data processing equipment (ADPE) and includes:

a. General and special purpose computers (e.g., digital, analog, or hybrid computer equipment);

b. Commercially available components, those produced as a result of research and development, and the equivalent systems created from them, regardless of size, capacity, or price, which are utilized in the creation, collection, storage, processing, communication, display, or dissemination of data;

c. Auxiliary or accessorial equipment, such as data communications terminals, source data automation recording equipment (e.g., optical character recognition equipment, paper tape typewriters, magnetic tape cartridge typewriters, and other data acquisition devices), data output equipment (e.g. digital plotters and computer output microfilmers), etc., to be used in support of digital, analog, or hybrid computer equipment, either cable-connected, wire-connected, or self-standing;

d. Electrical accounting machines used in conjunction with or independently of digital, analog or hybrid computers; and

e. Computer equipment which supports or is integral to a weapons system. [Ref. 35]

ANNUAL LOSS EXPENTANCY (ALE). The ALE of an ADP system or activity is the expected yearly dollar value loss from the harm to the system or activity by attacks against its assets.

ASSET. Any software, data, hardware, administrative, physical, communicatins, or personnel resource within an ADP system or activity. See ADP RESOURCES.

ATTACK. The realization of a threat. How often a threat is realized depends on such factors as the location, type, and value of information being processed. Thus, short of moving the system or facility or radically changing its mission, there is usually no way that the level of protection can affect the frequency of attack. The exceptions to this are certain human threats where effective security measures can have a deterrent effect. The fact that an attack is made does not necessarily mean that it will succeed. The degree of success depends on the vulnerability of the system or activity and the effectiveness of existing countermeasures.

AUDIT. To conduct the independent review and examination of system records and activities in order to test for adequacy of system controls, to ensure compliance with established policy and operational procedures, and to recommend any indicated changes in controls, policy, or procedures.
a. Internal Security Audit. An audit conducted by personnel responsible to the management of the orgainzation being audited.
b. External Security Audit. An audit conducted by an organization independent of the one being audited. [Ref. 36]

BROWSING. The act of searching through storage to locate or acquire information without necessarily knowing the existence or the format of the information being sought.

CENTRAL COMPUTER FACILITY. One or more computers with their peripheral and storage units, central processing units, and communications equipment in a single controlled area. This does not include remote computer facilities, peripheral devices, or terminals which are located outside the single controlled area, even though they are connected to the central computer facility by approved communication links. [Ref. 37]

CENTRAL SYSTEM OPERATOR. A system user who by virtue of security access control authorization has access to the user mode and the central system operator mode of the command interpreter. [Ref. 13]

COMMUNICATIONS SECURITY. The protection resulting from all measures designed to deny unauthorized persons information of value which might be derived from the possession and study of telecommunications, or to mislead unauthorized persons in their interpretation of the results of such possession and study. Also called COMSEC. Communications security includes cryptosecurity, transmission security, emission security, and physical security of communications security materials and information.

CONFIGURATION MANAGEMENT. The use of procedures appropriate for controlling changes to a system's hardware and software structure for the purpose of insuring that such changes will not lead to decreased data security.

CONTINGENCY PLANS. A plan for emergency response, backup operations, and post-disaster recovery maintained by an ADP activity as a part of its security program. A comprehensive

consistent statement of all the actions (plan) to be taken before, during, and after a disaster (emergency condition), along with documented, tested procedures which, if followed, will ensure the availability of critical ADP resources and which will facilitate maintaining the continuity of operations in an emergency situation.

COUNTERMEASURE. See section II.A.4.

DATA INTEGRITY. The state that exists when computerized data is the same as that in the source documents and has not been exposed to accidental or intentional modification, disclosure, or destruction. [Ref. 36]

DATA LEVEL.
Level I. Classified data.
Level II. Unclassified data requiring special protection; for example, Privacy Act, For Official Use Only, technical documents restricted to limited distribution.
Level III. All other unclassified data.

DATA SECURITY. The protection of data from unauthorized (accidental or intentional) modificaiton, destruction, or disclosure. [Ref. 36]

DESIGNATED APPROVING AUTHORITY (DAA). An official assigned responsibility to accredit ADP elements, activities, and networks under the official's jurisdiction.

ESCORT(S). Duly designated personnel who have appropriate clearances and access authorizations for the material contained in the system and are sufficiently knowledgeable to understand the security inplications of and to control the activities and access of the individual being escorted. [Ref. 37]

HARDWARE SECURITY. Computer equipment features or devices used in an ADP system to preclude unauthorized accidental or intentional modification, disclosure, or destruction of ADP resources.

MATERIAL. "Material" refers to data processed, stored, or used in and information generated by an ADP system regardless of form or medium, e.g., programs, reports, data sets or files, records, and data elements. [Ref. 35]

NEED-TO-KNOW. The necessity for access to, knowledge of, or possession of certain information required to carry out official duties. Responsibility for determining whether a person's duties require that possession of or access to such information and whether the individual is authorized to receive it rests upon the individual having current possession, knowledge, or control of the information involved and not upon the prospective recipient(s).

NETWORK. The interconnection of two or more ADP central computer facilities that provides for the transfer or sharing of ADP resources. The ADP network consists of the central computer facilities, the remote terminals, the interconnecting communication links, the front-end processors, and the telecommunications systems.

OPERATING SYSTEM (O/S). An integrated collection of service routines for supervising the sequencing and processing of programs by a computer. Operating systems control the allocation of resources to a user and their programs and play a central role in ensuring the secure operation of a computer system. Operating systems may perform debugging, input-output, accounting, resource allocation, compilation, storage assignment tasks, and other "system" related functions. Synonymous with terms such as "Monitor," "Executive," "Control Program," and "Supervisor." [Ref. 35]

PASSWORD. A protected word or string of characters that identifies or authenticates a user for access to a specific resource such as a data set, file, or record.

PERSONAL DATA. Data about an individual including, but not limited to, education, financial transactions, medical history, qualifications, service data, criminal or employment history which ties the data to the individual's name, or an identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph.

PERSONNEL SECURITY. The procedures established to ensure that each individual has a background which indicates a level of assurance of trustworthiness which is commensurate with the value of ADP resources which the individual will be able to access.

PHYSICAL SECURITY. Physical security is the protection of a material entity (property) from disruption of its safe and secure state and is concerned with physical measures designed to safeguard personnel, to prevent unauthorized access to equipment, facilities, material, and documents, and to safeguard them against espionage, sabotage, damage, and theft.

a. The use of locks, badges, and similar measures to control access to the central computer facility.

b. The measures required for the protection of the structures housing the central computer facility from damage by accident, fire, environmental hazards, loss of utilities, and unauthorized access.

REVIEW AND APPROVAL. The process whereby information pertaining to the security and integrity of an ADP activity or network is collected, analyzed, and submitted to the appropriate DAA for accreditation of the activity or network.

RESOURCE-SHARING COMPUTER SYSTEM. A computer system which uses its resources, including input/output (I/O) devices, storage, central processor (arithmetic and logic units), control units, and software processing capabilities, to enable one or more users to manipulate data and to process co-resident programs in an apparently simultaneous manner. The term includes systems with one or more capabilities commonly referred to as timesharing, multiprogramming, multi-accessing, multi-processing, or concurrent processing. [Ref. 35]

RISK. See section II.A.1.

RISK ANALYSIS (ASSESSMENT). An analysis of system assets and vulnerabilities to establish an expected loss from certain events based on estimated probabilities of the occurrence of those events. The purpose of a risk assessment is to determine if countermeasures are adequate to reduce the probability of loss or the impact of loss to an acceptable level.

SECURITY ACCESS CONSTRAINTS. The process and file access restrictions imposed by the security requirements. [Ref. 13]

SECURITY FILE. File containing user ids and associated access constraints. [Ref. 13]

SECURITY LOG. Data file containing violations of the security requirements. [Ref. 13]

SECURITY OFFICER. Designated individual who is responsible for maintaining the security procedures for the installation. [Ref. 13]

SECURITY INSPECTION. An examination of an ADP system to determine compliance with ADP security policy, procedures, and practices.

SECURITY SPECIFICATIONS. A detailed description of the countermeasures required to protect an ADP activity or network from unauthorized (accidental or intentional) disclosure, modification, and destruction of data, or denial of service.

SECURITY TEST AND EVALUATION (ST&E). An examination and analysis of the security features of an ADP activity or network as they have been applied in an operational environment to determine the security posture of the activity or network upon which an accreditation can be based.

SECURITY VIOLATION. Any attempt to gain access to the operating system, the operating system files and executable modules, or system user files and executable modules. [Ref. 13]

SENSITIVE BUSINESS DATA. Data which requires protection under Title 18, USC 1905, and other data which by its nature requires controlled distribution or access for reasons other than the fact that it is classified or personal data. Sensitive Business Data is recognized in the following categories:

a. For Official Use Only--Requiring confidentiality of information derived from Inspector General, authority, or other investigative activity.

b. Financial--Requiring protection to ensure the integrity of funds or other fiscal assets.

c. Sensitive Management--Requiring protection to defend against the loss of property, material, or supplies or to defend against the disruption of operations or normal management practices, etc.

d. Proprietary--Requiring protection to protect data or information in conformance with a limited rights agreement or which is the exclusive property of a civilian corporation

or individual and which is on loan to the Government for evaluation or for its proper use in adjudicating contracts.
e. Privileged--Requiring protection for conformance with business standards or as required by law. (Example: Government-developed information involving the award of a contract.)

SPLICE CONFIGURATION. An integrated set of six hardware/software systems required to achieve the functional, performance and capacity requirements of the SPLICE specifications. [Ref. 13]

SPLICE LOCATION. One or more SPLICE configurations in the same geographical area (on the same Local Computer Network) connected to Government-furnished equipment and interfaces. [Ref. 13]

SPLICE NETWORK. Provides the connectivity between geographically distant SPLICE locations. Government furnished data communications lines shall connect the locations through common carrier lines and/or through a Government-furnished network. [Ref. 13]

THREAT. See section II.A.2.

USER. A person or organization receiving products or services produced by a ADP system either by access to the system or by other means.

USER ID. Data element input to identify a system user and to label processing products resulting from the user-initiated processing. [Ref. 13]

VULNERABILITY See section II.A.3.

APPENDIX C
DEFENSE DATA NETWORK

This Appendix provides a short summary of the Defense Data Network (DDN). The source document used is the Defense Data Network Program Plan revised May 1982 [Ref. 38].

A. GENERAL DESCRIPTION

The DDN will be an integrated packet-switching data network designed to satisfy all DOD data networks requirements projections through the 1990's. The DDN will take advantage of existing networks, notably the WWMCCS Intercomputer Network (WIN) and the Advanced Research Projects Agency Network (ARPANET), and will be based primarily on ARPANET technology. Table X lists the standard components to be used in the DDN.

TABLE X

Standard DDN Components

Switching node hardware
Switching node software
Cryptographic devices
Mini-TACs
Host front-end devices
Host interface devices
Multiplexors

There will be 171 switching nodes located at about 85 widely distributed sites. The switching node is a Bolt Baranek and Newman (BBN) C/30, a microprogrammed

minicomputer costing about $45,000 (including TEMPEST/HEMP protection). The C/30 is designed for unattended operations. All switching nodes will be located on military facilities and secured to at least the SECRET level. The network will have a principle System Monitoring Center (SMC), an alternate SMC, regional Monitoring Centers (MCs) in Europe and the Pacific, and MCs for each separate community.

The DDN provides for increased survivability in several ways. The 171 fixed switching nodes and 9 fixed MCs will have HEMP protection (EM shielding, line isolation, and surge arresting protection). Sites with no backup power will be provided uninterruptable power supplies (UPS). There will be five prepositioned mobile reconstruction nodes equipped with MC capability. A dynamically adaptive routing algorithm will automatically route traffic around congested, damaged, or destroyed switches and trunks. Additionally, a dense trunking grid will provide redundancy at all possible points in the network.

There will be at least 99% availability between any pair of single-homed users. Critical subscribers will be dual-homed (a single access line to two switching nodes), providing at least 99.5% availability. Dual access lines to a single node can also be used.

Precedence levels can be assigned by originating hosts and terminals, and will be used in the allocation of network resources. Switching nodes provide for four levels of precedence, with preemption of lower precedence communications. Category I (FLASH and FLASH-OVERRIDE) communications will be processed in non-blocking mode exclusive of all other traffic modes and volumes.

Communications errors will be minimized by the use of error detection and correction mechanisms. A Cyclical Redundancy Check (CRC) of 16 bits is associated with host

messages on the access lines and packets on trunks. A 32 bit CRC is used with SIP-compatible hosts. Additionally, 16 bit checksums are provided on an end-to-end basis within the switch subnetwork and on a user-to-user basis via the Transmission Control Protocol (TCP). Error detection and correction hardware is used in the switches for protecting against memory failures and for checksumming of critical data structures and portions of code.

B. SPECIFIC DDN HARDWARE/SOFTWARE

1. Switching Node

The BBN C/30 packet switching processor is a multi-board, microprogrammed minicomputer, with 64k words of random access memory (RAM), which supports a full range of synchronous and asynchronous I/O interfaces. The C/30 software is the ARPANET Interface Message Processor (IMP) program which can be loaded locally (from a cassette) or downline loaded from a MC. The software provides the following functional capabilities:

- Store and forward traffic processing.
- Host access and end-to-end traffic processing (with a variety of host access protocols, see p. 33 of Ref. 38).
- Dynamic, adaptive, distributed routing which measures actual packet delays and routes individual packets along the least delay path.
- Monitoring and control services.

2. Internet Private Line Interface

The Internet Private Line Interface (IPLI) is a security device, currently under development as part of the Gray Tree program, which will be used for end-to-end encryption. It is composed of three functional units: a KG 84

cryptographic device and two MC68000 based packet processors (one on each side of the KG 84). Figure C.1 shows the placement of the IPLI with each host for end-to-end encryption on the DDN. The software in each processor will be based on the CMOS operating system, with the basic functions necessary for the DOD standard internet environment and monitoring and control functions. The protocol interfaces conform to the DOD Standard Internet Protocol (IP). Since the packet processing occurs at the lower level of the IP, the TCP and other protocols which exist above the IP can be supported.

Exclusive of the KG 84, the estimated unit cost for production IPLIs (after FY84) in lots of 100 or more is $15,000.

3. Mini-TAC

A mini-TAC is a terminal access device that allows a cluster of up to 16 synchronous and asynchronous terminals access to the network. It is logically equivalent to a network host and will use the same host-host protocols. The ARPANET-based mini-TAC software allows a terminal to connect to hosts on the network. The mini-TAC software multiplexes all the terminal-host connections over a single link between it and the switching node. Since Mini-TACs will not initially provide dial-up access, access will be over hard-wired lines and controlled by physical access control measures.

The mini-TAC will be constructed around a Motorola MC68000 microprocessor with memory, 16 synchronous or asynchronous terminal ports, and multiple network interface ports (to allow dual-homing). The mini-TAC will meet TEMPEST and HEMP requirements. Mini-TACs will communicate with other network hosts using DOD standard TCP and IP. Terminal level support is provided via the Telnet protocol.

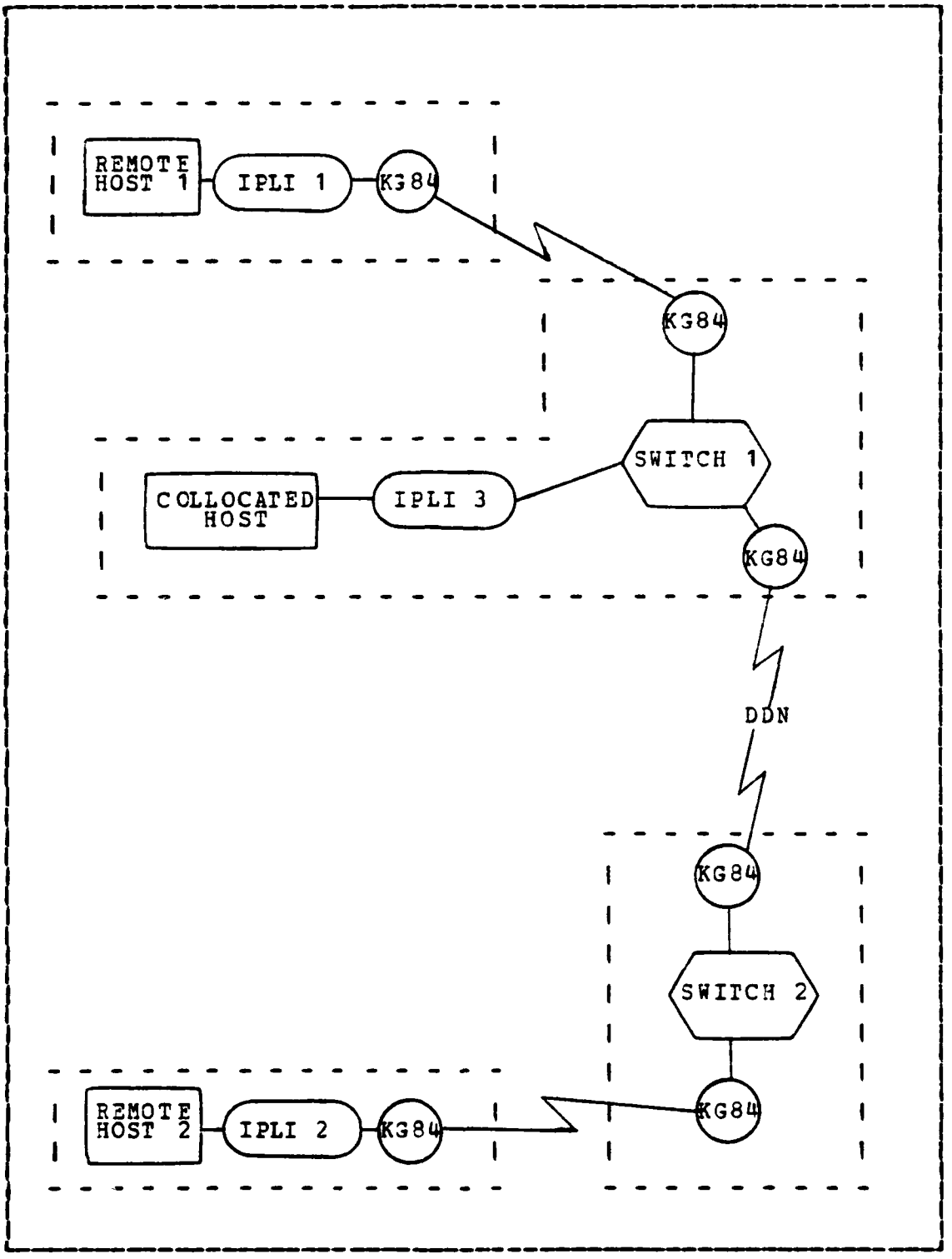


Figure C.1 End-to-end Encryption.

The mini-TAC will be designed for unattended operations. Control functions and hardware and software fault diagnosis can be done remotely from a Monitoring Center. Repair will be by board swapping. In quantities of 100, the production cost per unit is estimated at $7500 plus $250 per port.

C. SECURITY FEATURES

1. Link Encryption

The KG 84 crypto device will be used on all back bone trunks, on all access lines to classified hosts, and on access lines to sites that act as MCs for the unclassified community. Because all hosts will use the IPLI described above, communications on the trunks will be "super encrypted." The link encryption will conceal traffic patterns and monitoring reports, which might yield traffic analysis information. It also protects MC-switch control traffic, which is important since this traffic includes downline loading of sensitive switch software.

2. Security Level Separation

Separation of subscribers operating at different system high levels is provided by the use of IPLIs (at least one IPLI key for each different system high level), creating at least one logical subnet for each security level. Since IP and subnet headers must be in the clear for packet processing within the switch, all switches are TEMPEST enclosed and in military facilities secured to at least the SECRET level. Establishment of logical subnets will guarantee against delivery of communications to any subscriber outside the subnet. This guarantee against misdelivery will be used to protect statistical reports from being delivered to any hosts other than an MC. Each MC and the fake host in

each switch that communicates with the MC will be members of the logical subnet. Additionally, only the SMC can retrieve and accumulate traffic statistics.

3. Separation of Communities of Interest

Communities of interest are subscriber groups which present an acceptable level or risk to each other and require a high level of interoperability. Separation of communities of interest is accomplished through the creation of logical subnets by cryptographic means, by software control, or both. For unclassified subscribers, the switches provide the ability to define logical subnets which restrict traffic to flow only among the members of that logical subnet. The number of subnets provided by the switches is currently limited to 16, but can be increased to 32 or 64.

Classified user communities will be separated by IPLI subnets (like-keyed IPLIs). Current policy limits IPLI separated communities of interest to 128 subscribers.

4. Individual Access Control

Access control to subscriber facilities is the responsibility of the subscribers themselves. The network will assure that access of one subscriber to another is controlled with respect to authorized security level and community of interest, but will not verify that an individual user (person or process) has valid access rights to that subscriber.

5. Personnel Clearances and Keys

All personnel with access to switches must be cleared to the SECRET level due to the traffic analysis potential. This clearance level also applies to all personnel at the MCs. Personnel manning an MC for a secure

subnet must be cleared to the level of the subnet subscribers. Crypto technicians will be required for keying the IPLIs for each community and for link KGs. The keying material for each IPLI community is available only at the IPLI sites. The keying material for the link KGs is available on a pairwise basis at the switch sites based on switch connectivity.

LIST OF REFERENCES

1. Wooldridge, S., Corder, C.R., and Johnson, C.R., Security Standards for Data Processing, John Wiley and Sons, 1973

2. General Accounting Office Report Number FGMSD 76-40, Managers Need to Provide Better Protection for Federal ADP Facilities, 10 May 1976

3. IBM Corporation Report Security Risk Assessment in Electronic Data Processing Systems, by Robert H. Courtney, Jr., Draft, June 1978

4. The Report of the Privacy Protection Study Commission, "Appendix 4: The Privacy Act of 1974: An Assessment," by David F. Linnowes, Chairman, U.S. Government Printing Office, July 1977

5. U.S. Senate Committee on Government Operations, Computer Abuse - Problems Associated With Computer Technology in Federal Programs and Private Industry, 94th Congress, 2nd Session, U.S. Government Printing Office, June 1976

6. U.S. Senate Committee on Government Operations, Staff Study of Computer Security in Federal Programs, 95th Congress, 1st Session, U.S. Government Printing Office, February 1977

7. Office of Management and Budget, Circular No. A-71, Transmittal Memorandum No. 1, Security of Federal Automated Information Systems, 27 July 1978

8. Office of Management and Budget, News Release No. OMB-29, OMB Information Office, 28 July 1978

9. DOD Directive 5400.11, Subject: Personal Privacy and Rights of Individuals Regarding Their Personal Records, 4 August 1975

10. OPNAVINST 5239.1A, Subject: Department of the Navy Automatic Data Processing Security Program, 3 August 1982

11. NAVSUPSYSCOM, Stock Point Logistics Integrated Communications Environment (SPLICE) Security and Risk Analysis Plan, 1 November 1980

12. Burch, John G., Jr., and Sardinas, Joseph L., Computer Control and Audit: A Total Systems Approach, John Wiley and Sons, 1978

13. Department of the Navy Solicitation Document N66032-82-R-0007, Acquisition of Stock Point Logistics Integrated Communications Environment (SPLICE) Automatic Data Processing Equipment (Hardware and Software) and Services, Undated

14. Deputy Secretary of Defense Frank C. Carlucci MEMORANDUM, Subject: AUTODIN II Termination, 2 April 1982

15. NAVSUPINST 5510.6A, Subject: Security Requirements for Automatic Data Processing (ADP) Systems, 23 May 1980

16. Hoffman, Lance J., Modern Methods for Computer Security and Privacy, Prentice-Hall, 1977

17. Department of Commerce, National Bureau of Standards, Federal Information Processing Standards Publication 65, Subject: Guideline for Automatic Data Processing Risk Analysis, 1 August 1979

18. Jacobson, Robert V., "Quantitative Risk Assessment of Data Processing Facilities," Selected Papers and Presentations From the U.S. Army Third Automation Security Workshop, pp. 223-236, 8-10 December 1980

19. Fitzgerald, Jerry, "EDP Risk Analysis Using Matrices," EDPACS, v. 9, no. 5, p. 1-7, November 1981

20. Carroll, John M., Computer Security, Security World Publishing, 1977

21. Pritchard, J. A., Computer Security: Risk Management in Action, NCC Publications, 1978

22. Tater, Frederick P., "System Threat Identification," Proceedings of the Computer Security and Privacy Symposium, pp. 31-37, Honeywell Information Systems, April 19-20, 1977

23. Canning, Richard G., "Risk Assessment for Distributed Systems," EDP Analyzer, v. 18, no. 4, April 1980

24. Department of Commerce, National Bureau of Standards, Federal Information Processing Standards Publication 83, Subject: Guideline on User Authentication Techniques for Computer Network Access Control, 29 September 1980

25. Shankar, K.S., "The Total Computer Security Problem," Advances in Computer System Security, edited by Rein Turn, Artech House, Inc., 1981

26. Berman, A., "How to Keep Terminal Users Honest," Data Communications, v. 9, no. 5, May 1980

27. Department of Commerce, National Bureau of Standards, Federal Information Processing Standards Publication 46, Subject: Data Encryption Standard, 15 January 1977

28. Denning, Dorothy E., Cryptography and Data Security, Addison-Wesley Publishing, 1982

29. Hsiao, D.K., Derr, D.S., and Madnick, S.E., Computer Security, Academic Press, 1979

30. Wood, C., Fernandez, E.B., and Summers, R.C., "Data Base Security: Requirements, Policies, and Models," IBM Systems Journal, v. 19, no. 2, 1980

31. Department of Commerce, National Bureau of Standards, Special Publication 500-33, Subject: Considerations in the Selection of Security Measures for Automatic Data Processing Systems, June 1978

32. MITRE Technical Report MTR-3999, History of Protection in Computer Systems by John D. Tangney, 15 July 1980

33. IBM Corporation Report Data Security and Data Processing, Volume 5, Study Results: TRW Systems, Inc., by G.E. Short, June 1974

34. Naval Postgraduate School Report NPS-54-82-003, Functional Design of a Local Area Network, by Dr. N.F. Schneidewind, December 1982

35. DOD Directive 5200.28, Subject: Security Requirements for Automatic Data Processing (ADP) Systems, 18 December 1972

36. Department of Commerce, National Bureau of Standards, Federal Information Processing Standards Publication 39, Subject: Glossary of Computer Systems Security, 15 February 1975

37. DOD 5200.28-M, Subject: ADP Security Manual: Techniques for Implementing, Deactivating, Testing, and Evaluating Secure Resource-Sharing ADP Systems, January 1973

38. Defense Communications Agency, Defense Data Network Program Plan, January 1982, revised May 1982

BIBLIOGRAPHY

Brafman, Marvin J., "Evaluating Computer Controls Using a Matrix Approach," EDPACS, v. 9, no. 6, December, 1981

Bussolati, U. and Martella G., "Treating Data Privacy in Distributed Processing," Information Management, v. 4, no. 6, December, 1981

Buttar, Javed I., Dittman, William L, and Herring, Catherine A., "A Generalized Security Mechanism for Small and Medium Scale Information Management Systems," presented at the IEEE Region V Conference, 1980

Campbell, Robert P. and Sands, Gerald A., "A Modular Approach to Computer Security Risk Management," AFIPS Conference Proceedings, v. 48, 1979

Cheheyl, M.H., Gasser, M., Huff, G.A., and Miller, J.A., "Verifying Security," Computing Surveys, v. 13, no. 3, September, 1981

Conway, R.W., Maxwell, W.L., and Morgan, H.L., "On the Implementation of Security Measures in Information Systems," Communications of the ACM, v.15, no. 4, April, 1972

Denning, Dorothy E. and Denning, Peter J., "Certification of Programs for Secure Information Flow," Communications of the ACM, v. 20, no. 7, July, 1977

Department of Commerce, National Bureau of Standards, Federal Information Processing Standards Publication 31, Subject: Guideline for Automatic Data Processing Security and Risk Management, June 1974

Department of Commerce, National Bureau of Standards, Federal Information Processing Standards Publication 41, Subject: Computer Security Guidelines for Implementing the Privacy Act of 1974, 30 May 1975

Department of Commerce, National Bureau of Standards, Special Publication 500-27, Subject: Computer Security and the Data Encryption Standard, 15 February 1977

Gladney, Henry M., Worley, Elton L., and Myers, James J., "An Access Control Mechanism for Computing Resources," IBM Systems Journal, v. 14, no. 3, 1975

Hoffman, Lance J., "Impacts of Information System Vulnerabilities on Security," AFIPS Conference Proceedings, v. 51, June, 1982

Lamport, Leslie, "Password Authentication with Insecure Communication," Communications of the ACM. v. 24, no. 11, November, 1981

Losonsky, Terrana M., Automated Information System Security (AISS): A Comparative Analysis of Risk Management Procedures, Masters Thesis, George Washington University, Washington, D.C., 1979

Martin, James, Security, Accuracy, and Privacy in Computer Systems, Prentice-Hall, 1973

Moulton, Rolf, "Prevention: Better Than Prosecution," Government Data Systems, November/December, 1981

Mueller-Schloer, Christian and Wagner, Neal R., "The Implementation of a Cryptography-based Secure Office System," AFIPS Conference Proceedings, v. 51, June, 1982

NAVCOMPTINST 7000.36, Subject: Financial Management Systems: Standard criteria for internal ADP control of, 4 February 1975

Nielsen, Norman R. and Ruder, Brian, "Computer System Integrity Safeguards," Proceedings of IFIP, v. 77, 1977

Perley, E. Harold, "Organizing the EDP Security Function," EDPACS, v. 8, no. 10, April, 1981

Stiegler, Helmut G., "A Structure for Access Control Lists," Software - Practice and Experience, v. 9., 1979

Turn, Rein, "Private Sector Needs for Trusted/Secure Computer Systems," AFIPS Conference Proceedings, v. 51, June, 1982

Turn, Rein, Ganies, R. S., and Glaseman, S., "Problem Areas in Computer Security Assessment," AFIPS Conference Proceedings, v. 46, 1977

Ware, Willis H., "Security, Privacy and National Vulnerability," presented at Honeywell Computer Security and Privacy Symposium, 7 April 1981

Woods, Helen M. and Kimbleton, Stephen R., "Access Control Mechanisms for a Network Operating System," AFIPS Conference Proceedings, v. 48, June, 1979

INITIAL DISTRIBUTION LIST

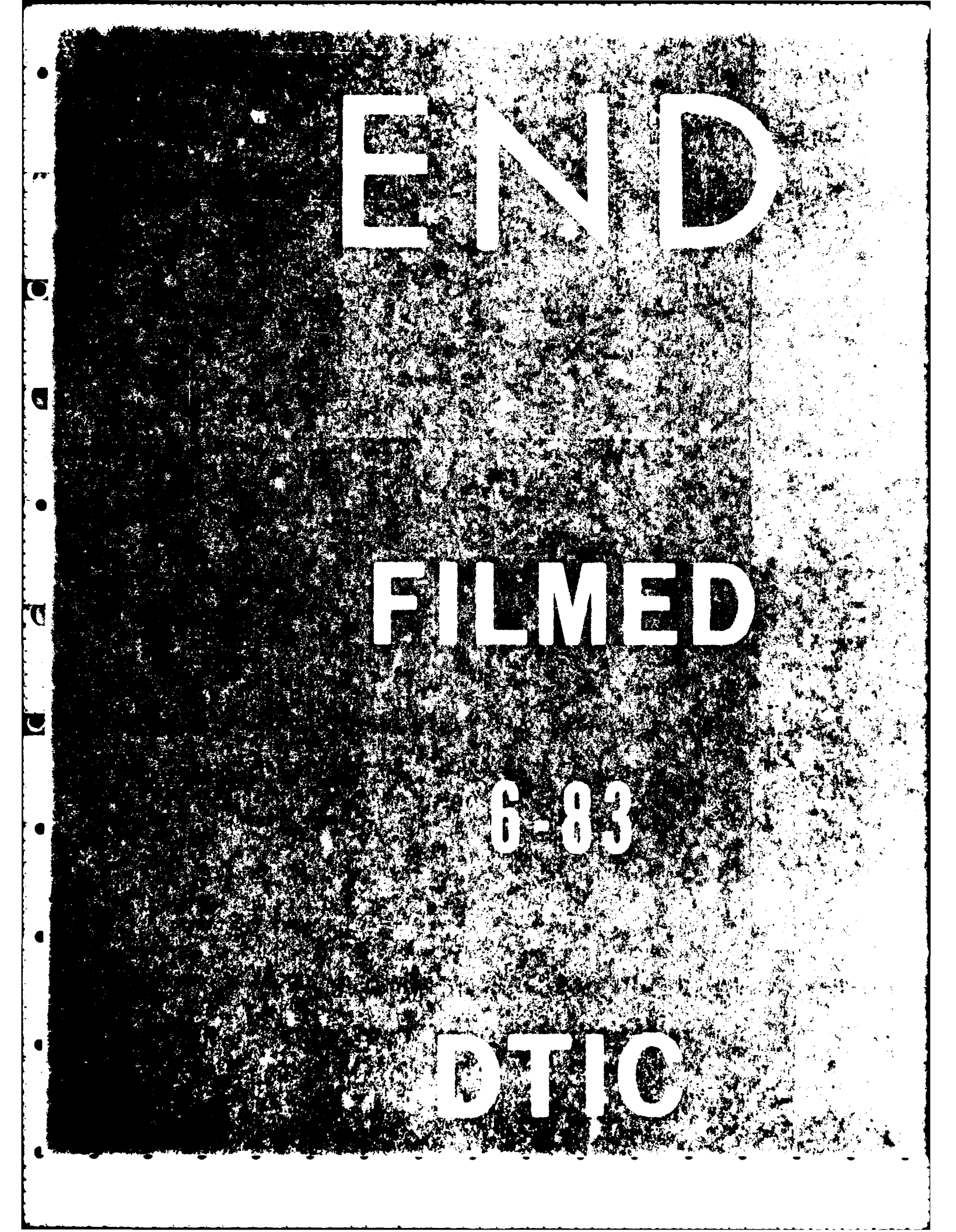
		No. Copies
1.	Defense Technical Information Center Cameron Station Alexandria, Virginia 22314	2
2.	Library, Code 0142 Naval Postgraduate School Monterey, California 93940	2
3.	Professor N.F. Schneidewind, Code 54SS Department of Administrative Sciences Naval Postgraduate School Monterey, California 93940	2
4.	LCDR John Hayes, Code 54HT Department of Administrative Sciences Naval Postgraduate School Monterey, California 93940	1
5.	Naval Postgraduate School Computer Technologies Curricular Office Code 37 Monterey, California 93940	1
6.	LT S.K. Crowder 3704 Lakota Road Alexandria, Virginia 22303	2
7.	LT J.M. Adams Tactical Training Group Atlantic FCTCL Dam Neck Virginia Beach, Virginia 23461	2
8.	Chief of Naval Operations CNO-942 Washington, D.C. 20350	1
9.	Commander Naval Data Automation Command Washington Navy Yard Washington, D.C. 20374	2
10.	Officer in Charge Navy Data Automation Facility Naval Air Station Lemoore Lemoore, CA 93245	1
11.	Commander, Naval Supply System Command LCDR Dana Fuller, Code 0415A Washington, D.C. 20379	1
12.	Fleet Material Support Office LT Ted Case, Code 942 Mechanicsburg, PA 17055	1
13.	Ms. Mary Willoughby P.O. Box 94 Mendocino, CA 95460	1

14. Major W.D. Helling 1
2511 Windsor Ave.
DuBuque, Iowa 52001

15. Commander, Naval Data Automation Command 1
Attn: Mr. Dick Fredette, Code 92
Bldg. 166
Washington Navy Yard
Washington, D.C. 20374

16. US Army Computer Systems Selection and 1
Acquisition Agency
Attn: MOSA-TDR Pat Malley
Rm 284, Hoffman 1
2461 Eisenhower Avenue
Alexandria, VA 22331

17. Command and Control Technical Center 1
Attn: C440 - Ms. Carol Giammo
11440 Isaac Newton Square North
Reston, VA 22090


END
FILMED
6-83
DTIC